NRIC VII

Network Reliability and Interoperability Council VII

Issue 3 –

September 2005

FOCUS GROUP 3B

Public Data Network Reliability

Final Report

About this Document

Per the NRIC VII Council Charter, the Public Data Network Reliability Focus Group planned three issues of its report as follows, with each issue intended to make vital information available to the communications industry as it became available.

- Issue 1, Gap Analysis Report. The first Issue contained information describing the results of a gap analysis of Best Practices aimed at the reliability of Internet data networks.

- Issue 2, Effectiveness Report. A second Issue was planned to include a survey of the effectiveness of the Best Practices for Internet data services. This work was completed on time per the charter schedule. However, the material was not published until Issue 3.

- Issue 3, Final Report. The Final Report recommends Best Practices for Internet data services providers, including the new Best Practices that particularly apply to public data network service providers.[1]

Each subsequent version integrates the newer material with that of the previous issue, and thus supersedes the earlier issues of this document.

[1] See footnote in Section 3.1.2, *Deliverables*, for additional information on this final deliverable.

Table of Contents

1 Results in Brief 5
1.1 Major Findings – Gap Analysis 5
1.2 Major Findings – Effectiveness Survey 6
1.3 Major Findings – Best Practices Definition 6
1.4 Summary of Conclusions and Recommendations 7
2 Objective, Scope, and Methodology 9
2.1 Objective 9
2.1.1 Mission 9
2.1.2 Deliverables 9
2.2 Scope 10
2.2.1 Scope Statement 10
2.2.2 Subject Matter 11
2.2.3 Network Types 11
2.2.4 Industry Roles 11
2.3 Methodology 12
2.3.1 Attributes of the Public Data Network 12
2.3.2 Best Practices 14
2.3.3 Specified Actions from the Focus Group 3B Mission Statement 16
2.3.4 Participants 16
2.3.5 Approach 18
2.3.6 Coordination with Other Stakeholders 22
2.3.7 Other Focus Groups 23
2.3.8 Non-Disclosure Agreement 23
3 Analysis and Findings 24
3.1 Gap Analysis 24
3.2 Task Group Analysis 24
3.2.1 ENVIRONMENT 26
3.2.2 HARDWARE 29
3.2.3 HUMAN 33
3.2.4 NETWORK 36
3.2.5 PAYLOAD 45
3.2.6 POLICY 48
3.2.7 POWER 53
3.2.8 SOFTWARE 56
3.3 Survey of Effectiveness 61
3.3.1 Additional Industry Engagement 61
3.3.2 Use of Third Party 61
3.3.3 Timeline 61
3.3.4 Approach 62
3.3.5 Survey Results 63
3.3.6 Other Observations 63
3.4 Best Practices 64
3.4.1 Best Practices and Previous Councils 65
3.4.2 Intended Use 65
3.4.3 Best Practice Search Options 66
3.4.4 General, Previous Council and Historic References 67
3.4.5 Best Practices Expressions 67
4 Conclusions 69

4.1 Gap Analysis 69
4.2 Effectiveness Survey 69
4.3 Public Data Network Best Practices.. 69
4.4 Areas for Further Investigation... 70
4.5 Summary 70
5 Recommendations 71
Appendix 1. List of Interviewees.. 72
Appendix 2. Bibliography and Documentation 74
Appendix 3. Acronyms 76
Appendix 4. NRIC VII Charter 78
Appendix 5. Public Data Network Attributes 87
Appendix 6. Public Data Network Gaps 91
Appendix 7. PDN Modifications of Existing Best Practices 93
Appendix 8. PDN New Best Practices... 97
Appendix 9. Acknowledgements 104

1 Results in Brief

The Charter of the Seventh Council dedicated part of its focus to Network Reliability. This Network Reliability focus includes two components: Wireless Networks and Public Data Networks. This is the Final Report of the Public Data Network Reliability Focus Group and presents three deliverables.

In fulfillment of the Charter's first deliverable description, the Focus Group completed an analysis that identifies gaps in existing, NRIC Best Practices for the reliability of the Public Data Network. Further, in fulfillment of its second prescribed deliverable, an industry survey on the effectiveness of these Best Practices was completed. Finally, to fulfill its third deliverable, the Focus Group modified existing Best Practices, and developed new Best Practices to address the specific needs of the Public Data Network (i.e., the "Services Applicability Improvement Process").

The Public Data Network Reliability Focus Group reports eight major accomplishments in this Final Report:

1. engagement of over 60 industry subject matter experts (Section 2 and 3)
2. articulation of over 70 attributes of the Public Data Network
3. consideration of over 200 concerns regarding the Public Data Network
4. formation of 8 Task Groups that provide systematic coverage of communications infrastructure elements (Section 3)
5. identification of 11 gaps in existing NRIC Best Practices (Section 3)
6. survey respondents on the effectiveness of the existing Best Practices serve over 95% of data subscribers (Section 3)
7. modification of 19 Best Practices to enhance their applicability to the Public Data Network (Section 3)
8. development of 45 new Best Practices to address the Public Data Network (Section 3)

1.1 Major Findings – Gap Analysis

The 11 gaps identified by this Focus Group were distributed across the infrastructure areas as follows:

Table 1.1. Distribution of Identified Gaps.

Area	Number of Gaps	Section
Environment	1	3.2.1
Hardware	0	3.2.2
Human	0	3.2.3
Network	4	3.2.4
Payload	0	3.2.5
Policy	0	3.2.6
Power	2	3.2.7
Software	4	3.2.8

Examples of identified gaps include:

Environment
The Environment Task Group identified one gap in existing NRIC Best Practices related to the complexity of managing growth in third party and multi-tenant environments (e.g., space, power, cooling).

Network
The Network Task Group has identified opportunities to enhance NRIC Best Practices in the following areas: network design, network management and measurement, maintenance window and spares administration.

Software
The Software Task Group has identified opportunities to enhance NRIC Best Practices in the area of crash diagnostic memory storage and the use of non-volatile memory. There is added opportunity to improve storage of core dumps and system states associated with a crash.

1.2 Major Findings – Effectiveness Survey

The NRIC VII Charter also directs that the Council should "… survey providers of public data network services, including Internet data services providers, concerning the efficacy of existing Best Practices." This survey was completed on time and with several improvements over previous NRIC surveys. The following statistics summarize the survey results:

- 52% increase in the number of survey respondents (compared to NRIC V survey)
- 97% of Best Practices included in the survey were rated as effective or moderately effective on average

Both the ratings and the comments provided by the respondents were studied by the Focus Group to determine what, if any, adjustments should be made to associated Best Practices.

In its analysis, the Focus Group observed that some Best Practices are identified by subject matter experts as being effective, and by other experts as being not applicable. This survey evidence further supports the principle that Best Practices are not applicable in all situations, as is stated throughout this report.

1.3 Major Findings – Best Practices Definition

Each of the Task Groups identified Best Practices by using the following three processes:

- Gap Closure Process
- Effectiveness Survey Process
- Public Data Network (PDN) Services Applicability Improvement Process

The total number of NRIC Best Practices that were identified by the eight Task Groups is summarized in the table below.

Table 1.3. Focus Group 3B PDN Summary of Best Practice Activities.

	Gap Closure Process (11 Gaps)	Effectiveness Survey Process	PDN Services Applicability Improvement Process	TOTAL
New Best Practices	26	0	19	**45**
Modified Best Practices	2	11	6	**19**
Deleted Best Practices	0	0	0	**0**

Section 3 provides a detailed discussion for each of the processes for each of the eight communications infrastructure areas.

Areas for Further Investigation

In addition to completing the deliverables directed by the Council Charter, the Focus Group reviewed its work to determine if there were any discoveries that went beyond its scope, but that were appropriate to present. One such item was identified. The Power Task Group identified the following issue as one that is emerging as increasingly critical to the reliability of public data network services:

> The subject of power for residential and business premises equipment should be considered in future work, primarily as it relates to access to essential services during commercial power outages [Section 3.2.7].

1.4 Summary of Conclusions and Recommendations

The Focus Group completed all deliverables on time and consistent with the direction of the Council Charter. This report documents highly valuable guidance for Service Providers, Network Operators and Equipment Suppliers that promotes reliability for the nation's Public Data Network.

Best Practice development depends on the contributions of many subject matter experts from a broad range of perspectives. This was effective because of the substantial time commitment of those engaged.

Going forward, industry participants are strongly encouraged to have their respective subject matter experts review these Best Practices for applicability. The NRIC web site (www.nric.org) Best Practices tools have keyword and other search capabilities that make identifying the list of applicable Best Practices to a given job function efficient. It is critical to note that Best Practices are not applicable in every situation because of multiple factors. Therefore, government entities are cautioned that mandating Best Practices could contribute to suboptimal network reliability or result in other negative consequences.

For example, Best Practices that recommend avoiding the placement of critical network facilities in high risk areas could, *if followed without appropriate consideration*, result in poor coverage. Similarly, a Best Practice that encourages deployment of certain types of back-up power, *if implemented inappropriately*, could result in a violation of local ordinances. And, likewise, a Best Practice that encourages the removal of foliage near infrastructure in some instances may result in deterioration or destruction of environmental aesthetics if proper discretion is not used.

With this understanding, the Focus Group has prepared the following recommendation for the Council to advance these Best Practices:

> **The Council recommends that the NRIC VII Public Data Network Reliability Best Practices be implemented, as appropriate, by Service Providers, Network Operators and Equipment Suppliers, in order to promote the reliability and robustness of the public data network throughout the United States.**

These Best Practices have been developed to assure optimal reliability and robustness under reasonably foreseeable circumstances. The scope of this activity also encompasses guidance that promotes the sustainability of communications networks throughout the United States; the availability of adequate communications capacity during events or periods of exceptional stress due to natural disaster, terrorist attacks or similar occurrences; and the rapid restoration of communications services in the event of widespread or major disruptions in the provision of communications services.

2 Objective, Scope, and Methodology

2.1 Objective

The Charter of the Seventh Council charged it to *"…[build] on the work of the previous Councils . . . to develop Best Practices and refine or modify, as appropriate, Best Practices developed by previous Councils aimed at improving the reliability of public data networks."* Specifically, the Charter stated, "The Council shall evaluate the applicability of all Best Practices that have been developed for public data network providers. The Council shall perform a gap analysis to determine areas where new Best Practices for these providers are needed. The Council shall survey providers of public data network services, including Internet data services providers, concerning the efficacy of existing Best Practices. The Council shall focus on the special needs of public data services providers and refine existing Best Practices to improve their applicability to Internet data services and other public data network services."

2.1.1 Mission

The Mission of the Focus Group 3B is derived directly from the NRIC VII Charter (Appendix 4). The Mission is almost verbatim from applicable sections of the Council Charter, with a few exceptions for clarification.

<u>Focus Group 3B Mission</u>

> **Building on the work of the previous Councils, as appropriate, this Council shall continue to develop Best Practices and refine or modify, as appropriate, Best Practices developed by previous Councils aimed at improving the reliability of public data networks. In addition, the Council shall address the following topics in detail.**
>
> **The Council shall evaluate the applicability of all Best Practices that have been developed for public data network providers. The Council shall perform a gap analysis to determine areas where new Best Practices for these providers are needed. The Council shall survey providers of public data network services, including Internet data services providers, concerning the efficacy of existing Best Practices. The Council shall focus on the special needs of public data services providers and refine existing Best Practices to improve their applicability to Internet data services and other public data network services.**

2.1.2 Deliverables

The Focus Group 3B deliverables, as defined by the NRIC VII Charter, are:

> **Interim Milestones**
> **By December 8, 2004, the Council shall provide a report describing the results of the gap analysis of Best Practices aimed at the reliability of Internet data services.**

By April 29, 2005, the Council shall complete its survey of the effectiveness of the Best Practices for Internet data services.

Final Milestone
By September 25, 2005, the Council shall provide a report recommending the Best Practices for Internet data services providers including the new Best Practices that particularly apply to public data network service providers.[2]

2.2 Scope

2.2.1 Scope Statement

In NRIC VII Focus Group 3B, a Public Data Network (PDN) is defined as a network established and operated for the specific purpose of providing data transmission services for the public. Such networks are considered ‘in scope' for Focus Group 3B.

The NRIC VII Focus Group 3B on Public Data Network Best Practices has classified its scope of coverage into three categories:

1. In Scope for Focus Group 3B:

   - guidance covering the configuration and operation of in-scope networks including general design characteristics, equipment, emergency use of network resources (but not E911), customer interfaces, the impact of government policy recommendations, and any general areas, such as power and security on which in-scope networks depend.

   - guidance covering inter-provider information and configuration including inter-provider routing configurations, Asynchronous Transfer Mode (ATM) and Frame Relay (FR) Network-to-Network Interface (NNI), NOC-to-NOC communication, abuse resolution and contact information management.

   - guidance covering formerly regulated services that are moving to unregulated PDNs that have specific requirements in the in-scope networks.

2. Out of Scope for Focus Group 3B:

   - non-US legal issues, private corporate network requirements and operations, inter-provider business or commercial relations and contracts (e.g., peering agreements and financial arrangements), provider Acceptable Use Policies, and users of networks.

[2] The FCC NRIC VII Designated Federal Officer (DFO) provided an interpretation to the Focus Group during its Meeting No. 7 (July 20-21, 2004 workshop in Washington DC). The DFOs guidance was that better wording for this third deliverable was as follows: “By September 25, 2005, the Council shall provide a report recommending the Best Practices for Internet data services providers including the new Best Practices that particularly apply *to service providers that use IP technology in the infrastructures*.”

- guidance directed at a specific vendor or service provider or recommendations to use specific vendors or services.

3. In Scope for Focus Group 3B discussion, but should be deferred to other NRIC Focus Groups:

    - guidance on general areas, such as power and security that do not have specific concerns for the in-scope networks.

2.2.2 Subject Matter

The subject matter is network reliability. Network interoperability and security are considered to the extent that they may impact network reliability.

2.2.3 Network Types

Network Types included are: Asynchronous Transfer Mode (ATM), Frame Relay (FR), Internet Protocol (IP) and related hybrid or other data protocols.

2.2.4 Industry Roles

The scope includes Service Providers, Network Operators, Equipment Suppliers and Property Managers of the public communication infrastructure. The following is a brief definition of the principal organizational components referred to throughout the NRIC Best Practices:[3]

Service Providers
An organization that provides services for content providers and for users of a computer network. The services may include access to the computer network, content hosting, server of a private message handling system, news server, etc. A company, organization, administration, business, etc., that sells, administers, maintains or charges for the service. The service provider may or may not be the operator of the network.

Network Operators
The operator is responsible for the development, provision and maintenance of real-time networking services and for operating the corresponding networks.

Equipment Suppliers
An organization whose business is to supply network operators and service providers with equipment or software required to render reliable network service.

Property Managers
The responsible party for the day-to-day operation of any facility (including rooftops and towers), usually involved at the macro level of facility operations and providing service to a communications enterprise. This responsibility may include lease management, building infrastructure operation and maintenance, landlord/tenant relations, facility standards compliance (such as OSHA, and common area maintenance and operation, which may include base building security and reception. Based on this definition, the use of "property manager" in a Best Practice would refer to the responsible operational entity, which may be the facility owner or "landlord",

[3] T1A1 Telecom Glossary: http://www.atis.org/tg2k

the majority owner of a shared facility (e.g., third party data center), the owner's representative, a professional property management company, a realty management company, tenant representative (in the case of triple net or like-kind lease arrangement), a facility provider, a facility manager, or other similar positions.

Government
Government includes federal, state and local entities.

2.3 Methodology

The methodology used by this Focus Group is largely based on doing what is needed to fulfill the applicable portions of the Council Charter, and drawing from industry experience to document what works well.

The Public Data Network Focus Group is one of two under the network reliability focus of the Seventh Council. In addition, the Seventh Council continued to pursue work addressed in previous Councils: Homeland Security and Broadband, as well as introducing a new focus on Emergency Communications Networks (Figure 2.3).

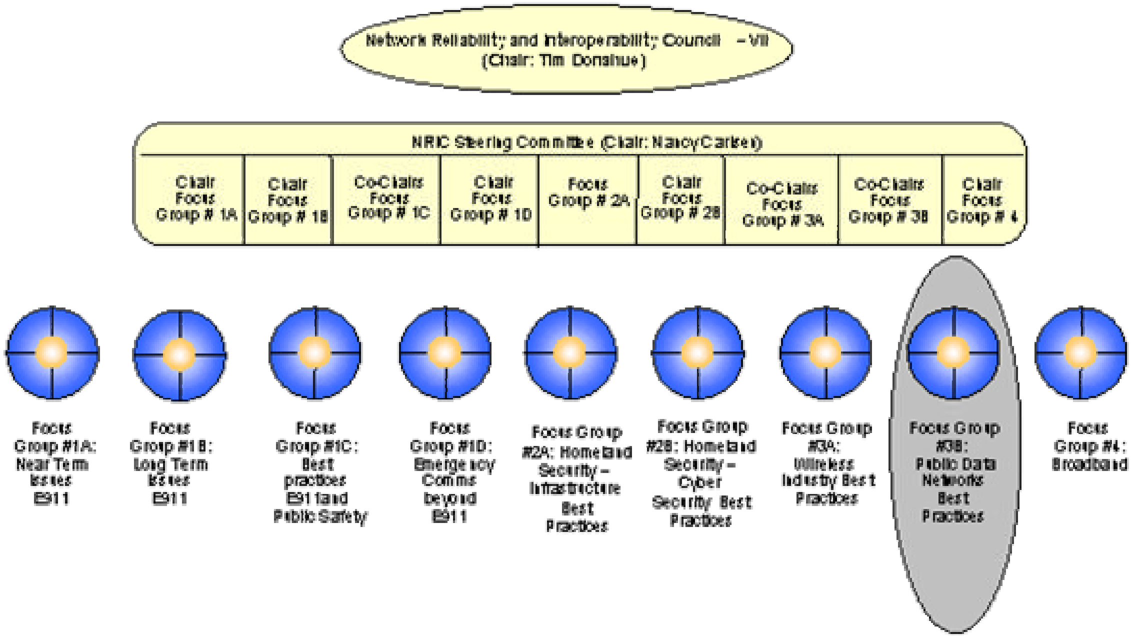

Network Reliability and Interoperability Council – VII
(Chair: Tim Donahue)
NRIC Steering Committee (Chair: Nancy Carter)
Chair Focus Group # 1A
Chair Focus Group # 1B
Co-Chairs Focus Group # 1C
Chair Focus Group # 1D
Focus Group # 2A
Chair Focus Group # 2B
Co-Chairs Focus Group # 3A
Co-Chairs Focus Group # 3B
Chair Focus Group # 4
Focus Group #1A: Near Term Issues E911
Focus Group #1B: Long Term Issues E911
Focus Group #1C: Best practices E911 and Public Safety
Focus Group #1D: Emergency Comms beyond E911
Focus Group #2A: Homeland Security – Infrastructure Best Practices
Focus Group #2B: Homeland Security – Cyber Security Best Practices
Focus Group #3A: Wireless Industry Best Practices
Focus Group #3B: Public Data Networks Best Practices
Focus Group #4: Broadband

Figure 2.3. NRIC VII Focus Group Structure.

2.3.1 Attributes of the Public Data Network

Previous Councils have increasingly included both the subject matter of data networks and then solicited the involvement of relevant expertise. For example, the Fifth Council included a Subcommittee on Packet Switching Best Practices. This Subcommittee reviewed all existing Best Practices to determine applicability to packet switching networks and services. Approximately 97% of the existing Best Practices were found to be applicable, most with some minor refinements or modifications.[4] The Sixth Council

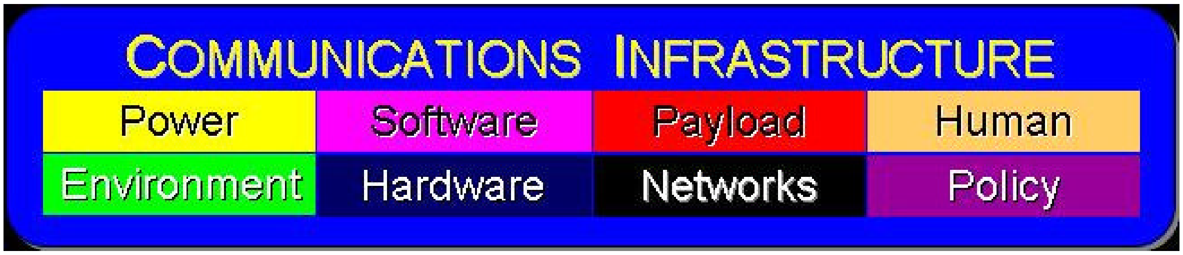
[4] NRIC V Packet Switching Network Reliability Subcommittee Final Report, January 2002, www.nric.org.

also included a focus on data networks. However, this Seventh Council brings an even further level of attention. Recognizing the substantial work available to this Focus Group from the previous Councils, the FCC Designated Federal Officer (DFO) requested that the Focus Group ensure sufficient new rigor was brought into the process. Specifically, the DFO asked the Focus Group to “start from scratch” in its understanding of the special needs of the Public Data Network.

To ensure healthy rigor in understanding the special needs of the Public Data Network, the Focus Group assembled a list of the attributes that need to be considered. The Focus Group generated a list of over 70 such attributes. A list of attributes of the Public Data Network is listed in Appendix 5.

The Focus Group then used this list of attributes along with the experience and perspectives of the membership to generate a list of concerns that could affect the reliability of the Public Data Network.

Each concern was then assigned to one of eight Task Groups representing the following areas of the communications network.



COMMUNICATIONS INFRASTRUCTURE

Power	Software	Payload	Human
Environment	Hardware	Networks	Policy

Figure 2.3.1.A. Eight Areas of the Communications Infrastructure.

The eight areas associated with these Task Groups provided comprehensive, systematic coverage of communications infrastructure.

Figure 2.3.1.B provides a set of pictures showing the Task Group in action.

Figure 2.3.1.B. Analysis of Concerns for the Public Data Network.

2.3.2 Best Practices[5]

Best Practices are statements that describe the industry's guidance to itself for the best approach to addressing a concern. NRIC Best Practices are the most authoritative list of such guidance for the communications industry. They result from unparalleled industry cooperation that engages vast expertise and considerable resources.

The implementation of specific Best Practices is intended to be voluntary. In addition, the applicability of each Best Practice for a given circumstance depends on many factors that need to be evaluated by individuals with appropriate experience and expertise in the same area addressed by the Best Practice. More information on the use of Best Practices is provided in Section 3.4.2, *Intended Use of Best Practices*. This section focuses on the factors considered in the *development* of the Best Practices. There are seven principles that are key to understanding the nature of NRIC Best Practices for the communications industry.[6]

[5] The term "Best Practices" is capitalized when referring to specific NRIC Best Practices.

[6] These principles were brought forward from the work of the NRIC V Packet Switching Network Reliability Best Practices Subcommittee and the NRIC VI Homeland Security Physical Security Focus Group.

1. “People Implement Best Practices”
The Best Practices are intended for daily use by the many thousands of individuals who support the communications infrastructure. To this end, the Best Practices address the following three values:

- applicability of Best Practices to individual job functions
- appreciation for the Value of Best Practices
- accessibility to appropriate Best Practices

Even though NRIC Best Practices have been developed to be easily understood, their essence is often not immediately apparent to those who are inexperienced with the associated job functions.[7] Therefore caution should be given to ensure that those managing Best Practices within organizations have sufficient experience.

2. Best Practices do not endorse commercial or specific "pay for" documents, products or services, but rather stress the essence of the guidance provided by such (e.g., formal quality management vs. "TL9000") practices. Helpful examples are identified in the "References Columns" available on the web site.

3. Best Practices are more effective and appropriate when they address (help prevent, mitigate, etc.) classes of problems. Detailed fixes to specific problems are not Best Practices.

4. Best Practices are already implemented by some, if not many, companies. Many fascinating and impressive ideas can be generated by the highly regarded list of organizations assembled for this effort. However, such ideas do not qualify as Best Practices if no one is “practicing them.” The recommended Best Practices being provided to the industry in this document have been demonstrated to be effective, feasible and capable of being implemented.

5. Best Practices are developed by industry consensus. In particular, the parties with “skin in the game” (i.e., Service Providers, Network Operators, and Equipment Suppliers) are able to bring their expertise from across the industry to weigh in on the “best” approach to addressing a concern.

6. Best Practices are verified by a broader set of industry members – from outside the Focus Group – to ensure that those who have not been a part of the process can provide feedback. For example, an industry survey was conducted in 2005.

7. Best Practices are presented to the industry only after sufficient rigor and deliberation has warranted the inclusion of both the conceptual issue and the particular wording of the practice. Discussions among experts and stakeholders include consideration of:

- Existing implementation level of a proposed Best Practice
- Effectiveness of a proposed Best Practice
- Feasibility to implement a proposed Best Practice

[7] Section 7, NRIC V Best Practices Subcommittee Final Report, January 2002. The Keywords provide associations between job functions and Best Practices.

- Risk not to implement a proposed Best Practice
- Alternatives to the proposed Best Practice

2.3.3 Specified Actions from the Focus Group 3B Mission Statement

The Focus Group 3B Mission Statement (Section 2.1.1) specifies 12 specific actions that are to be undertaken by the Focus Group.

1. shall continue to develop Best Practices
2. shall refine Best Practices
3. shall modify Best Practices
4. shall address the following topics [refers to items 5 through 9]:
5. shall evaluate the applicability of the PDN Best Practices
6. shall perform a gap analysis to determine areas for new PDN Best Practices
7. shall survey PDN and Internet Service Providers on the efficacy of existing Best Practices
8. shall focus on the special needs of PDN Service Providers
9. shall refine existing Best Practices for PDN and Internet Services
10. shall provide a report on Best Practice Gaps for Internet data services
11. shall complete its survey of the effectiveness of the Best Practices for Internet data services
12. shall provide a report recommending Best Practices for Internet data services applicable to IP Service Providers

2.3.4 Participants

This section provides a brief description of the Focus Group membership's strong industry representation and activities. For approximately 25% of the organizations, their participation in this Focus Group effort was their first experience in an NRIC effort.

2.3.4.1 Industry Representation

The participants represented a balance across the industry roles (i.e., service providers, equipment suppliers, industry forums, government, others). Figure 3, *Public Data Network Focus Group*, lists the participating organizations and their representatives. In addition to the Focus Group members, additional experts were engaged with these organizations and from other organizations to support the Task Group activities described in Section 3.2.

The Focus Group also included a diverse array of disciplines with formal training and experience ranging from mathematics, psychology, field experience, public policy, computer science, human performance, network operations, finance, physics, theology, business management as well as various fields of engineering. In addition, Focus Group members regularly consulted others within their organizations.

PUBLIC DATA NETWORK RELIABILITY - FOCUS GROUP 3B

Co-Chair: David Frigeri*, Internap
Co-Chair: Karl F. Rauscher*, Lucent Technologies Bell Labs

SERVICE PROVIDERS, NETWORK OPERATORS

ALLTEL	Scott Binns Tim Hall*	**Nextel**	KC Kim*
AT&T	Rick Canaday	**Qwest**	Brian Rooks
BellSouth	Jim L. Johnson	**RCN**	Joe Provo
CenturyTel	Brent Austin Brian White	**SBC**	John Chapa Ren Provo
Comcast Cable	Dean Brewster*	**Sprint**	Chase Cotton*
Cox Communications	Mark Adams*	**Telefonica**	Dennis Di Toro
Equinix	William Norton	**Time Warner Cable**	Ron da Silva
Internap	Duke McMillin* Jon Vestal	**Verizon**	Robin Howard
Intelsat	Mark Neibert		
MCI	Barry Briggs Mike Diorio		

EQUIPMENT SUPPLIERS

Cisco Systems	Robin Roberts	**Lucent Technologies**	Richard Krock* James P. Runyon*
Juniper Networks	Fred Stringer*		

OTHERS

ATIS	Bill Klein (A)	**Harvard University**	Scott Bradner
CTIA	Rick Kemper	**Quality & Reliability Solutions, LLC**	Brad Nelson*
FCC	Jeff Goldthorp (A) Kent Nilsson (A)	**SAIC**	Hank Kluepfel (A)
		Telcordia Technologies	Spilios Makris

***Task Group Leaders**
(A) Advisors
Figure 2.3.4.1. Public Data Network Reliability Focus Group.

2.3.4.2 Activities

The membership was very active. Specific activities include researching issues, engaging internal and external experts, coordinating internal reviews of draft materials, completing action items and preparing for meetings. Section 2.3.5.2, *Meeting Logistics*, provides statistics on the aggregate participant-hours associated with meetings.

Representatives were typically supported by several subject matter experts within their respective organizations.

2.3.5 Approach

The Focus Group's approach to fulfill its Mission was based on the steps of assembling sufficient expertise and diversity of perspectives, generating a list of PDN attributes, developing a list of concerns from this list of attributes and the assembled expertise and then conducting analysis to determine if the known concerns are covered by existing NRIC Best Practices. To do this, several meetings were dedicated to brainstorming and rigorous discussion with respect to the following areas:

Attributes of PDN and Internet Service Provider Networks
- Over 70 PDN and ISP attributes were identified by this activity (Appendix 5)

Issues and concerns faced by PDNs and Internet Service Provider Networks
- Over 200 issues and concerns were identified by this activity

Priority topics that the PDN Focus Group should consider
- 11 gaps were identified (Appendix 6)

Effectiveness Survey
- 11 Best Practices were modified based on survey feedback

Services Applicability Improvement Process
- 6 existing Best Practices were modified
- 19 new Best Practices were developed

Using the eight dimensions of the communications infrastructure identified in Figure 2.3.5, the Focus Group formed Task Groups. The PDN and ISP attributes, issues and problems, and priority topics were distributed across these Task Groups, as appropriate.

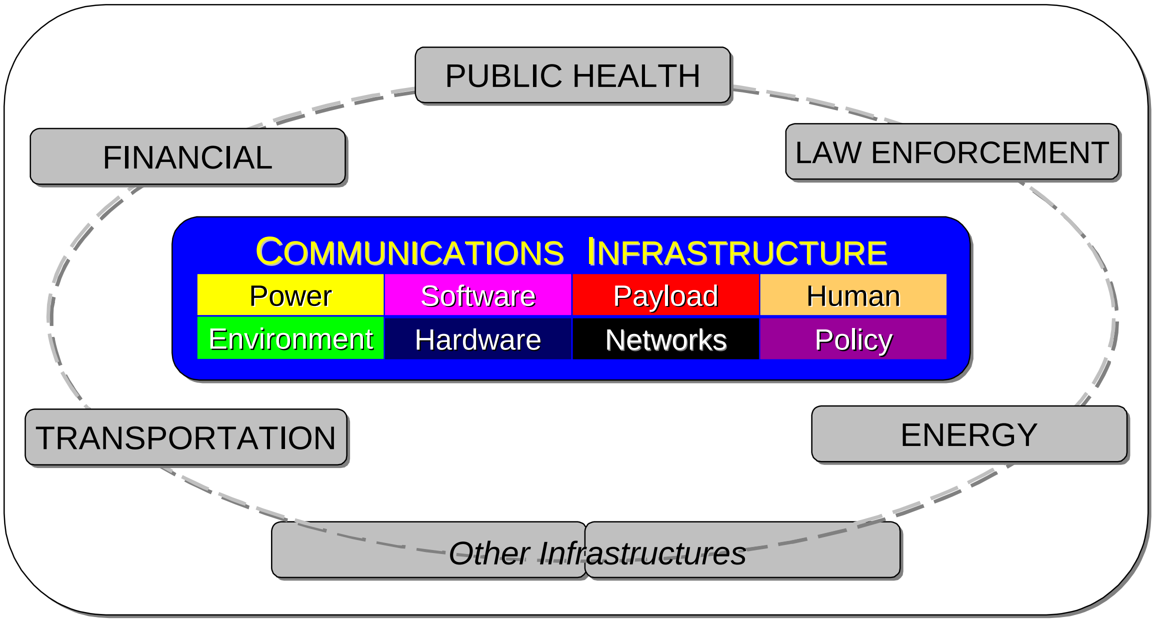


Figure 2.3.5. Communications Infrastructure.[8]

[8] From NRIC VI Homeland Security Physical Security Focus Group.

The Task Groups and Leaders are as follows:

- Environment Task Group – Dean Brewster, Comcast Communications; Jim Runyon, Lucent Technologies-Bell Labs
- Hardware Task Group – Tim Hall, ALLTEL; Karl Rauscher, Lucent Technologies-Bell Labs; Fred Stringer, Juniper Networks
- Human Task Group – KC Kim, Nextel Communications
- Network Task Group – Mark Adams, Cox Communications
- Payload Task Group - David Frigeri, Internap Network Services
- Policy Task Group – Chase Cotton, Sprint
- Power Task Group – Rick Krock, Lucent Technologies-Bell Labs
- Software Task Group – Brad Nelson, Quality & Reliability Solutions, LLC

2.3.5.1 Key Elements

There were two elements of the approach used by the Focus Group that allowed it to achieve industry-level agreements.

Consensus

A key element of the approach is that the consensus of broad industry representation articulated the Focus Group's output. This commitment to consensus greatly increased the amount of time required to agree on the Focus Group's output. However, the resulting confidence and quality are invaluable to the industry.

Protection of Sensitive Information

The Focus Group leaders encouraged all members to discuss vulnerabilities in their essence and avoid specifics, unless necessary. In addition, the Focus Group's materials and discussions were treated as confidential. A Non-Disclosure Agreement was made available by the Steering Committee Chair and signed by many of the members. This allowed participants to engage their peers with even greater protection of sensitive information.

2.3.5.2 Meeting Logistics

The Focus Group set an aggressive meeting schedule. Summary Statistics for the meeting scheduled from May 2004 through September 2005 are shown in Table 2.3.5.2.A.

Table 2.3.5.2A. Meeting Statistics.

Meeting Type	Participant-Hours
Conference Call	~ 650
Workshops	~1550
Total	**~2200**

In addition to the meeting participation time, each of the eight Task Groups had numerous meetings that accounted for hundreds of additional hours of meetings.

Table 2.3.5.2B provides the dates of each of the Focus Group meetings, indicates whether the meeting was a conference call or workshop and the number of participants at the meeting. Note that some of these meetings lasted 2 days.

Table 2.3.5.2.B. Focus Group Meetings and Participation.

2004 MEETINGS Focus Group 3B Public Data Networks			
MEETING NUMBER	DATE	MEETING TYPE	PARTICIPANTS
1	May 13, 20024	Conference Call	26
2	May 21, 2004	Conference Call	20
3	May 25, 2004	Workshop (DC)	16
	May 26, 2004	Workshop (DC)	16
4	June 7, 2004	Conference Call	19
5	June 25, 2004	Conference Call	19
6	July 16, 2004	Conference Call	19
7	July 20, 2004	Workshop (DC)	14
	July 21, 2004	Workshop (DC)	13
8	August 3, 2004	Conference Call	15
9	August 25, 2004	Conference Call	21
10	September 8, 2004	Workshop (DC)	15
	September 9, 2004	Workshop (DC)	13
11	September 20, 2004	Conference Call	16
12	October 4, 2004	Workshop (DC)	15
	October 5, 2004	Workshop (DC)	13
13	October 18, 2004	Conference Call	13
14	November 3, 2004	Workshop (DC)	8
	November 4, 2004	Workshop (DC)	10
15	November 8, 2004	Conference Call	10
16	November 9, 2004	Conference Call	11
17	November 10, 2004	Conference Call	12
18	November 11, 2004	Conference Call	13
19	November 12, 2004	Conference Call	11
20	November 15, 2004	Conference Call	7
21	December 14, 2004	Conference Call	16
22	December 23, 2004	Conference Call	5

2005 MEETINGS

Focus Group 3B – Public Data Networks

MEETING NUMBER	DATE	MEETING TYPE	PARTICIPANTS
23	January 7, 2005	Conference Call	15
24	January 14, 2005	Conference Call	15
25	January 21, 2005	Conference Call	14
26	January 28, 2005	Conference Call	14
27	February 2, 2005	Workshop (DC)	16
	February 3, 2005	Workshop (DC)	12
28	February 18, 2005	Conference Call	15
29	March 2, 2005	Workshop (DC)	12
	March 3, 2005	Workshop (DC)	8
30	March 18, 2005	Conference Call	14
31	April 12, 2005	Workshop (DC)	15
	April 13, 2005	Workshop (DC)	13
32	May 10, 2005	Workshop (DC)	13
33	June 2, 2005	Conference Call	14
34	June 8, 2005	Workshop (DC)	13
	June 9, 2005	Workshop (DC)	12
35	June 20, 2005	Conference Call	12
36	July 13, 2005	Workshop (DC)	12
37	July 26, 2005	Conference Call	12
38	August 3, 2005	Workshop (DC)	13
39	August 11, 2005	Conference Call	15
40	August 18, 2005	Conference Call	10
41	August 23, 2005	Conference Call	16

2.3.5.3 Guiding Principles for Members

The work of this Focus Group was the result of tremendous contributions from many organizations. In order to effectively work together, the team agreed to the following principles at the first face-to-face meeting:[9]

1. **The Work is Critical and Urgent**
   … Successful completion of our mission is vital to national security, economic stability and public safety
2. **High Quality, On-Time Deliverables that are Trustworthy and Thorough**
   … Fulfill applicable Charter requirements and meet the needs of the Nation
3. **Clear Objectives**
   …. For team, and individual participants and organizations
4. **Leadership Will Pursue Consensus of Team**
   … Also needs to set pace & guide fulfillment of charter
5. **Follow a Scientific Approach, Not Merely Collect Subjective Opinions**
   … Be objective and practice a disciplined methodology
6. **Capture Every Good Idea**
   … Welcome new and different perspectives for consideration
7. **Respect for Individuals**
   … Open and honest interactions

2.3.6 Coordination with Other Stakeholders

In order to avoid unnecessary duplication of effort and to better realize synergies, the leaders of NRIC and other key entities have appropriately agreed to coordinate their activities. Government and industry stakeholders include the following organizations and their constituents:

- Alliance for Industry Solutions (ATIS)
  - Network Reliability Steering Committee (NRSC)
- American National Standards Institute (ANSI)
- Cellular Telecommunications and Internet Association (CTIA)
- Institute of Electrical and Electronics Engineers (IEEE)
  - Communications Society (COMSOC)
  - Technical Committee on Communications Quality & Reliability (CQR)
- International Engineering Consortium (IEC)
- Internet Engineering Task Force (IETF)
- International Telecommunications Union (ITU)
- National Association of Regulatory Utility Commissioners (NARUC)
- National Institute of Standards and Technology (NIST)
- National Telecommunications and Information Administration (NTIA)
- North American Network Operators' Group (NANOG)
- President's National Infrastructure Advisory Council (NIAC)
- President's National Security Telecommunications Advisory Committee (NSTAC)
- United States Department of Homeland Security
  - National Communications System (NCS)
  - National Coordinating Center for Telecommunications (NCC)
  - Telecom ISAC (Information Sharing and Analysis Center)
- United States Telecommunications Association (USTA)

[9] These principles are carried forward from NRIC V and VI.

2.3.7 Other Focus Groups

Because of the common areas of subject matter, the Public Data Network Reliability Focus Group needed to coordinate some activities. Liaisons were established between this Focus Group and each of the other NRIC VII Focus Groups.

Special coordination was required with the following Focus Groups in order to resolve conflicting Best Practice recommendations submitted by each Focus Group (FG). These Focus Groups were: FG 2A “Homeland Security - Infrastructure,” FG 2B “Homeland Security - Cyber Security,” and FG 3A “Wireless Network Reliability.”

2.3.8 Non-Disclosure Agreement

A Non-Disclosure Agreement was prepared by the NRIC VII Steering Committee to provide additional protection for parties that may bring sensitive information to the Focus Group for discussion.

3 Analysis and Findings

3.1 Gap Analysis

The 11 gaps identified by this Focus Group were distributed across the communications infrastructure areas as shown in Table 3.1.

Table 3.1. Distribution of Identified Gaps

Area	Number of Gaps	Section
Environment	1	3.2.1
Hardware	0	3.2.2
Human	0	3.2.3
Network	4	3.2.4
Payload	0	3.2.5
Policy	0	3.2.6
Power	2	3.2.7
Software	4	3.2.8

These gaps are described in detail in the Task Group reports in the following sub-sections. Further, the mechanism used for the closure of each of these gaps (e.g., new Best Practices) is also described.

3.2 Task Group Analysis

A Task Group was formed for each of the eight communications infrastructure areas. The number of new, modified or deleted Best Practices identified by each Task Group is identified in the following table.

Table 3.2.A. Focus Group 3B Task Group Best Practice Summary.

	ENVIRONMENT	HARDWARE	HUMAN	NETWORK	PAYLOAD	POLICY	POWER	SOFTWARE	TOTAL
New Best Practices	2	5	3	20	1	5	0	9	45
Modified Best Practices	0	4	0	14	0	0	1	0	19
Deleted Best Practices	0	0	0	0	0	0	0	0	0

The following table provides the total number of new, modified or deleted Best Practices that were identified by each of the three processes used by each of the eight Task Groups. These processes are:

- PDN Gap Closure Process
- PDN Effectiveness Survey Process.
- PDN Services Applicability Improvement Process

Table 3.2.B. Focus Group 3B Best Practice Summary.

	Gap Closure Process (11 Gaps)	Effectiveness Survey Process	PDN Services Applicability Improvement Process	TOTAL
New Best Practices	26	0	19	**45**
Modified Best Practices	2	11	6	**19**
Deleted Best Practices	0	0	0	**0**

3.2.1 ENVIRONMENT

3.2.1.1 Environment Subject Matter

Everything needs to be somewhere. Environment includes a wide range of areas such as buildings, tower sites, satellite glide paths, cable trenches, ocean floors and overhead lines. Communications infrastructure is virtually everywhere.

Some environments present many challenges to communications equipment. Considerations such as temperature, fire, contaminates, floods, ice, snow, and animals, such as birds and rodents, are addressed in this area. Some factors related to the environment can be controlled or mitigated and some cannot, making the task of protecting communications infrastructure an incredible challenge.

The Environment Task Group reviewed reliability considerations of the Public Data Network by addressing the design, planning, construction, growth, access, and operations related to environments.

3.2.1.2 Environment Task Group Participants

The Environment Task Group assembled a diverse team of 9 individuals with representatives that include equipment suppliers, network operators and service providers. In addition to members of the Task Group, subject matter experts were engaged to strengthen its expertise and develop proposed Best Practices. Table 3.2.1.2 lists the Environment Task Group participants.

Table 3.2.1.2. Environment Task Group Participants.

Name	Organization
Victor DeVito	AT&T
Dean Brewster, ***Leader***	Comcast Corporation
Ray Cruz	Internap Network Services
Jim Runyon, ***Leader***	Lucent Technologies-Bell Labs
Rick Krock	Lucent Technologies-Bell Labs
Brad Nelson	Quality & Reliability Solutions, LLC
Brian Rooks	Qwest Communications
Molly Schwarz	Schwarz Consulting
Chase Cotton	Sprint

3.2.1.3 Environment Summary

The Environment Task Group methodology was to develop Best Practices by identifying and closing gaps, through the evaluation of the results of the Effectiveness Survey, and via the PDN service applicability process. The following table summarizes the results of the Best Practices resulting from these activities. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

Table 3.2.1.3 - Environment Task Group Summary of Best Practice Activities.

	Gap Closure Process (1 Gap)	Effectiveness Survey Process	PDN Services Applicability Improvement Process	TOTAL
New Best Practices	2	0	0	**2**
Modified Best Practices	0	0	0	**0**
Deleted Best Practices	0	0	0	**0**

3.2.1.4 Environment Gap Analysis

The Council Charter directs the Focus Group to "…*perform a gap analysis to determine areas where new Best Practices for [the Public Data Network] providers are needed*."

As a starting point and to encourage free form and innovative thinking the Focus Group and Environment Task Group used brainstorming and analysis methods or submittals by industry experts to detail a listing of nine potential concerns for the environment area of the Public Data Network.

The nine potential concerns were subsequently analyzed by the Environment Task Group to determine if they were applicable to the Public Data Network and potential candidates for a Best Practice Guidance. Through this analysis, the original list was consolidated into a more concise grouping of five potential concerns. These concerns underwent detailed analysis and a review against current Best Practices to determine the proper disposition. These five concerns were determined to be: 1) addressed by existing Best Practices, 2) transferred to the Homeland Security Infrastructure Focus Group, or 3) identified as gaps for Public Data Network reliability.

Managing Growth in Multi-Tenant Facilities

The Environment Task Group identified one gap in existing, NRIC Best Practices[10] related to the complexity of managing growth in third party and multi-tenant environments (e.g., space, power, cooling).

3.2.1.5 Environment Gap Closure

NRIC VI identified over 90 Best Practices[11] that are applicable to Property Managers of multi-tenant facilities. The following two new NRIC Best Practices have been defined to address the gap that was identified by the Environment Task Group.

- **7-P-5282** Service Providers should coordinate with Property Managers to ensure adequate growth space.

[10] An NRIC Best Practices web site search for the various areas of expertise under study revealed the following forty Best Practices as applicable to the environmental issues and items: 6-6-5072, 6-6-5073, 6-6-1004, 6-5-0599, 6-6-5207, 6-6-1067, 6-5-0655, 6-5-0699, 6-6-5204,6-6-5214, 6-6-5232, 6-6-5275, 6-5-0597, 6-5-0588, 6-6-1001, 6-6-0577, 6-6-8068, 6-6-5259, 6-6-1020, 6-6-1051, 6-6-5138, 6-6-5139, 6-6-5064, 6-6-5119, 6-6-5006, 6-6-5008, 6-6-5021, 6-6-5011, 6-6-5012, 6-6-5026, 6-5-0723, 6-5-0651, 6-5-0652, 6-6-5120, 6-6-5149, 6-6-5229, 6-6-5239, 6-5-0658, 6-6-5197, 6-6-5145

[11] Obtained via the NRIC VI Best Practice web site using text search with 'Property Manager'.

- **7-P-5283** Equipment Suppliers should provide network element thermal specifications or other special requirements in order to properly size Heating, Ventilation, and Air Conditioning (HVAC) systems.

3.2.1.6 Environment Effectiveness Survey Process

The Environmental Best Practices selected for the Effectiveness Survey were rated effective or moderately effective and, as such, no modifications were identified (see Table 3.2.1.3).

3.2.1.7 Environment Services Applicability Improvement Process

Per the NRIC VII charter, the PDN Focus Group was to “refine existing Best Practices to improve their applicability to Internet data services and other public data network services.”

The Task Group was assigned issues of concern, some of which were identified as gaps in existing Best Practices (see Section 3.2.1.4). For the Environment Task Group, all the identified issues were addressed by existing Best Practices.

3.2.1.8 Environment Issues for Further Investigation

Based on scope and known processes in place, there were no issues identified by the Environment Task Group that will require further investigation.

3.2.2 HARDWARE

3.2.2.1 Hardware Subject Matter

Hardware plays a fundamentally critical role in the reliability of the public data network. The hardware area includes the broad category of physical electronics and related components that are part of communications systems. Hardware systems include: frames, racks, cabinets, chassis; circuit packs, cards, blades, plug-ins and modules; fiber optic transmission facilities; cables (with exception to the power systems and power distribution systems such as fuse panels, which are addressed in the Power Section 3.2.7). The electronic hardware equipment includes switches, routers, multiplexing equipment, transmission equipment, access equipment, satellites, dishes, undersea cables, microwave repeaters, cell sites, etc. There are on the order of tens of thousands of routers and switches from multiple equipment suppliers deployed in U.S. public networks. These network elements range in size from something as small as a cereal box to complexes of more than 10 cabinets. Sometimes a carrier hotel contains many service providers using switches and routers from many different equipment suppliers.[12]

3.2.2.2 Hardware Task Group Participants

The Hardware Task Group assembled a team of sufficient expertise to effectively address the hardware subject matter as it relates to the reliability of the public data network. The Hardware Task Group was made up of 13 participants. In addition to members of the Focus Group, the Task Group engaged other subject matter experts to strengthen its expertise. The primary hardware disciplines of physics, chemistry and electrical engineering were represented on the team. Table 3.2.2.2 lists the Hardware Task Group participants. Care was also taken to include representation from a broad range of industry roles as well as from different technologies. The team had sufficient expertise to complete this activity.

Table 3.2.2.2. Hardware Task Group Participants.

Name	Organization
Tim Hall	ALLTEL
Jim Johnson	BellSouth
Robin Roberts	Cisco Systems
Mark Adams	Cox Communications
Scott Bradner	Harvard University
Duke McMillan	Internap Network Services
Fred Stringer, ***Leader***	Juniper Networks
Brad Nelson	Quality & Reliability Solutions, LLC
KC Kim	Nextel Communications
Rick Krock	Lucent Technologies-Bell Labs
Theodore Lach	Lucent Technologies
Karl Rauscher, ***Leader***	Lucent Technologies-Bell Labs
Hank Kluepfel	SAIC

[12] Network Reliability and Interoperability Council (NRIC) VI Homeland Security Physical Security Focus Group Final Report, Issue 3, December 2004, p. 49 (www.nric.org).

3.2.2.3 Hardware Summary

The Hardware Task Group identified areas of potential concern and reviewed the existing Best Practices in the subject area to identify gaps and potential improvements.

The following table summarizes the results of the Best Practices resulting from these activities. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

Table 3.2.2.3. Payload Task Group Summary of Best Practice Activities.

	Gap Closure Process (0 Gap)	Effectiveness Survey Process	PDN Services Applicability Improvement Process	TOTAL
New Best Practices	0	0	5	**5**
Modified Best Practices	0	2	2	**4**
Deleted Best Practices	0	0	0	**0**

3.2.2.4 Hardware Gap Analysis

The Council Charter directs the Focus Group to *"…perform a gap analysis to determine areas where new Best Practices for Public Data Networks providers are needed."* As described in Section 2.3.5, the approach used by the Hardware Task Group was similar for the other areas. Therefore, a gap is here defined as a space between the known problems associated with hardware that can impact network reliability and the existing NRIC Best Practices for hardware. To understand the former boundary, a list was generated of 19 known concerns for hardware. To understand the latter boundary, the existing Best Practices were researched and 54 were found to have potential application to the reliability of the public data network.[13] In addition, the Task Group reviewed the work of the previous Council in which the vulnerabilities of hardware were systematically reviewed. [14, 15] The Task Group's gap analysis determined that there were no significant gaps in the hardware area.

[13] An NRIC Best Practices web site keyword search for "hardware" returns the following 54 Best Practices: 6-5-0501, 6-5-0504, 6-5-0510, 6-5-0541, 6-5-0548, 6-5-0553, 6-5-0554, 6-5-0557, 6-5-0559, 6-5-0590, 6-5-0600, 6-5-0614, 6-5-0618, 6-5-0620, 6-5-0622, 6-5-0657, 6-5-0664, 6-5-0699, 6-5-0702, 6-5-0745, 6-5-0749, 6-5-0750, 6-6-1066, 6-6-5030, 6-6-5061, 6-6-5064, 6-6-5080, 6-6-5081, 6-6-5082, 6-6-5083, 6-6-5084, 6-6-5085, 6-6-5086, 6-6-5088, 6-6-5098, 6-6-5117, 6-66-5118, 6-6-5119, 6-6-5148, 6-6-5149, 6-6-5171, 6-6-5194, 6-6-5195, 6-6-5198, 6-6-5200, 6-6-5202, 6-6-5219, 6-6-5230, 6-6-5237, 6-6-5245, 6-6-5262, 6-6-5277, 6-6-5278, 6-6-5279.

[14] Vulnerability: *A characteristic of any aspect of the communications infrastructure that renders it, or some portion of it, susceptible to damage or compromise.* NRIC VI Homeland Security Physical Security Focus Group Final Report, Issue 3, December 2003, p. 39.

[15] The Homeland Security Physical Security Focus Group (1A) of NRIC VI carefully listed the *categories* of hardware vulnerability as chemical, physical, electromagnetic, environmental and life cycle (aging). The specific vulnerabilities include corrosion, temperature, shock, vibration, physical destruction, radiation and aging. These vulnerabilities, if exercised by a threat, can shorten the life or cause intermittent malfunctioning of hardware systems, or in the extreme, shut them down. See NRIC VI Homeland Security Physical Security Focus Group Final Report, Issue, 3, December 2003, p. 49.

3.2.2.5 Hardware Gap Closure

While there were no gaps identified in the Issue 1 report of this document, modifications were made to existing Best Practices to include PDN.

3.2.2.6 Hardware Effectiveness Survey Process

The Hardware Task Group reviewed the Effectiveness Survey which resulted in the modification of two Best Practices. The modified Best Practices from the Effectiveness Survey are:

- **7-P-0614** **Equipment Identification:** Service Providers, Network Operators and Equipment Suppliers should position the equipment designation information (e.g., location, labels, RFID tags) so that they are securely affixed. The equipment designation should not be placed on removable parts such as covers, panels, doors, or vents that can be removed and mistakenly installed on a different network element.

- **7-P-5084** **Hardware & Software Quality Assurance:** Service Providers, Network Operators and Equipment Suppliers should consider ensuring that outsourcing of hardware and software includes a quality assessment, functional testing and security testing by an independent entity.

  Reference: Independent entities do not include the source supplier. Quality and security testing may include the following: GR929 (RQMS), GR815, TL9000.

3.2.2.7 Hardware Services Applicability Improvement Process

There were 20 areas of concern identified during the Gap Analysis. These concerns resulted in the following new and modified Best Practices.

New Best Practices: The following new Best Practices are proposed for PDNs:

- **7-P-0419** **Capacity Management Systems:** Service Providers should design and capacity-manage EMSs (Element Management Systems) and OSSs (Operational Support Systems) to accommodate changes in network element capacity.

- **7-P-0420** **Management Systems Performance:** Network Operators should periodically measure EMS (Element Management System), NMS (Network Management System) and OSS (Operational Support System) performance and compare to a benchmark or applicable requirements to verify performance objectives and expectations (e.g., internal performance criteria, system vendor specifications) are being met.

- **7-P-0421** **Fast Failover of Redundancies:** Equipment Suppliers should design network elements intended for critical hardware and software recovery mechanisms to minimize restoration times.

  Reference: Common recovery mechanisms could include the fail-over to: a) the redundant hardware components (modules, FRUs), b) redundant and/or backup software processes, c) switch to alternate paths, circuits or virtual circuits, and, d) switch to redundant or backup storage of system data.

- **7-P-0423 Cable Management:** Equipment Suppliers should provide cable management features and installation instructions for network elements that maintain cable bend radius, provide strain relief and protection from cable damage, while also leaving clear access for cable rearrangement (i.e., moves/add/deletes) and FRU (Field Replaceable Unit) swaps.

- **7-P-0424 Electrical Safety Standards:** Network Operators should identify and require applicable safety standards for network elements that they plan to purchase, procure or implement. Recognized standards should be used where ever possible, with specific requirements cited rather than statements such as UL Listed or NEC compliant.

  Reference: Recognized standards may include UL, NEC, ANSI, NFPA, ASTM. Specific requirements such as "UL-498/NEC-250.146(A)-Receptacle Grounding-Surface-Mounted Box.”

Modified Best Practices: The following Best Practices are modifications to existing NRIC Best Practices:

- **7-P-0517 Equipment Control Mechanisms:** Equipment Suppliers should design network elements and associated network management elements with the combined capability to dynamically handle peak load and overload conditions gracefully and queue and shed traffic as necessary (e.g., flow control).

  Reference: The management of peak load and overload conditions can apply to bearer traffic, signaling traffic, routing and control protocol traffic, network management traffic/messaging, accounting statistics, and flow reporting.

- **7-P-0519 Capacity Monitoring:** Network Operators and Service Providers should engineer and monitor networks to ensure that operating parameters are within capacity limits of their network design (e.g., respect limitations of deployed packet switches, routers and interconnects, including "managed networks" and "managed CPE"). These resource requirements should be re-evaluated as services change or grow.

3.2.2.8 Hardware Issues for Further Investigation

Based on scope and known processes in place, there are, for the hardware area, no items identified for further investigation.

3.2.3 HUMAN

3.2.3.1 Human Subject Matter

The human element plays a critical role in the reliability of the public data network. This area includes employees of network operators, carriers, equipment suppliers, government, and property managers who are associated with the development, deployment and management of public data network communications systems. Many network related problems are caused by or affected by human interactions. Items considered within the human area include preventing human errors, protecting humans, the tendency of humans to resist change, sharing experiences about events involving humans, determining sound processes and procedures, providing training, educating customers, and sharing proper information within the society. There are over 1,000,000 people working in various companies associated with the U.S. public data network. The size, structure and organizational culture of each company play an important role in determining the degree of network exposure to human vulnerabilities.

3.2.3.2 Human Task Group Participants

The Human Task Group assembled a team of sufficient expertise to effectively address the human subject matter as it relates to the reliability of the public data network. The Human Task Group was made up of four participants. In addition to members of the Focus Group, the Task Group engaged other subject matter experts to strengthen its expertise. Table 3.2.3.2 lists the Human Task Group participants. The team had sufficient expertise to complete this activity.

Table 3.2.3.2. Human Task Group Participants.

Name	Organization
Anil Macwan	Lucent Technologies
Michael Diorio	MCI
KC Kim, ***Leader***	Nextel Communications
Ren Provo	SBC

3.2.3.3 Human Summary

The Human Task Group methodology was to develop Best Practices by identifying and closing gaps, identifying PDN service applicability and implementing the results of the Effectiveness Survey. The following table summarizes the outcome of the Best Practices resulting from these activities. Subsequent sub-sections will provide additional details for each of the activity defined in the methodology.

Table 3.2.3.3. Human Task Group Summary of Best Practice Activities.

	Gap Closure Process (0 Gap)	Effectiveness Survey Process	PDN Services Applicability Improvement Process	TOTAL
New Best Practices	0	0	3	**3**
Modified Best Practices	0	0	0	**0**
Deleted Best Practices	0	0	0	**0**

3.2.3.4 Human Gap Analysis

The Council Charter directs the Focus Group to "…*perform a gap analysis to determine areas where new Best Practices for [the Public Data Network] providers are needed*."

As a starting point and to encourage free form and innovative thinking, the Focus Group and Human Task Group used brainstorming and analysis methods or submittals by industry experts to detail a listing of eight potential concerns for the human area of the public data network.

The eight potential concerns were subsequently analyzed by the Human Task Group to determine if they were applicable to the public data network and potential candidates for Best Practice Guidance. These concerns underwent detailed analysis and review against current Best Practices to determine the proper disposition. These concerns were either: 1) determined to be addressed by existing Best Practices, 2) transferred to the Network, Software, and Hardware Task Groups, or 3) identified as gaps for Public Data Network reliability.

The Human Task Group identified no significant gaps in existing, NRIC Best Practices related to the human area. The Human Task Group generated three new Best Practices for PDN Services Applicability Improvement Process.

3.2.3.5 Human Gap Closure

NRIC VI identified over 81 human Best Practices[16] that are applicable to employees and employee training. The Human Task group did not find any serious gaps in the existing Best Practices as shown in Table 3.2.3.3.

3.2.3.6 Human Effectiveness Survey Process

The Human Best Practices selected for the Effectiveness Survey were rated effective or moderately effective and, as such, no modifications were identified.

3.2.3.7 Human Services Applicability Improvement Process

Per the NRIC VII charter, the PDN Focus Group was to "refine existing Best Practices to improve their applicability to Internet data services and other public data network services."

[16] An NRIC Best Practices web site keyword search for "human" returns the following 9 Best Practices: 6-5-0561, 6-5-0564, 6-5-0650, 6-5-0678, 6-5-0746, 6-5-5027, 6-5-5059, 6-5-5061, 6-6-5086. An NRIC Best Practices web site keyword search for "employee" returns the following 20 Best Practices: 6-5-0542, 6-5-0570, 6-5-0598, 6-5-0697, 6-5-0716, 6-6-1016, 6-6-1018, 6-6-1038, 6-6-5015, 6-6-5016, 6-6-5019, 6-6-5033, 6-6-5037, 6-6-5115, 6-6-5164, 6-6-5244, 6-6-8098, 6-6-8100, 6-6-8519, 6-6-8521. An NRIC Best Practices web site keyword search for "training" returns the following 61 Best Practices: 6-5-0511, 6-5-0537, 6-5-0564, 6-5-0565, 6-6-0577, 6-5-0578, 6-5-0579, 6-5-0588, 6-5-05896-5-0597, 6-5-0598, 6-6-0599, 6-5-0629, 6-5-0650, 6-5-0697, 6-5-0711, 6-5-0713, 6-5-0729, 6-6-1001, 6-6-1019, 6-6-1035, 6-6-1036, 6-6-1057, 6-6-3212, 6-6-5015, 6-6-5019, 6-6-5021, 6-6-5023, 6-6-5027, 6-6-5054, 6-6-5055, 6-6-5067, 6-6-5091, 6-6-5093, 6-6-5094, 6-6-5114, 6-6-5115, 6-6-5116, 6-6-5126, 6-6-5138, 6-6-5139, 6-6-5155, 6-6-5175, 6-6-5178, 6-6-5179, 6-6-5184, 6-6-5203, 6-6-5208, 6-6-5217, 6-6-5244, 6-6-5266, 6-6-5267, 6-6-5269, 6-6-5270, 6-6-8062, 6-6-8067, 6-6-8082, 6-6-8097, 6-6-8100, 6-6-8517, 6-6-8519

The Task Group was assigned issues of concern and no significant gaps in existing Best Practices (see Section 3.2.3.4) were identified. Other issues required actions to be taken to create new Best Practices.

The following three new Best Practices have been defined to improve PDN service applicability.

- **7-P-0434** **Employee Training:** Service Providers, Network Operators, Equipment Suppliers and Property Managers should provide appropriate training and periodic refresher courses for their employees.

- **7-P-0435** **ID Network Reliability Functions:** Service Providers, Network Operators, Equipment Suppliers and Property Managers should assess the functions of their organization and identify those critical to ensure network reliability.

- **7-P-0436** **Problem Handling Continuity:** Service Providers should have a process to ensure smooth handling and clear ownership of problems that transition shifts or organizational boundaries.

3.2.3.8 Human Issues for Further Investigation

Based on scope and known processes in place, there were no issues identified by the Human Task Group that will require further investigation.

3.2.4 NETWORK

3.2.4.1 Network Subject Matter

A Network is defined as a series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain sub-networks. The networks that support the United States communications infrastructure are immense both in terms of communications services provided and geographic coverage. Networks are designed with capabilities that minimize or mitigate the impact of failures on the services provided. A public data network is for the specific purpose of providing data transmission services for the public. At the network level, environment, power, hardware, software, human, procedure and policy must all come together to form a reliable communications infrastructure. The Network Task Group is focused on improving the reliability of the public data network by addressing the design and planning, provisioning, operations, administration and maintenance aspects of network performance:

Design and Planning: The activities associated with building, expanding or modifying a network. Examples include capacity management, planning and implementing network design, engineering of new facilities and routes.

Provisioning: The creation of subscriber account or the modification of parameters associated with the account. Provisioning of a subscriber account includes subscriber account registration and device activation.

Operations: The day-to-day activities associated with keeping a network operating reliably and efficiently. Examples include traffic management, circuit grooming and other activities centered on improving or ensuring network performance.

Administration: Administration includes all activities associated with managing a network from a business, network and information technology perspective (e.g., billing, IP address administration, databases).

Maintenance: The ongoing corrective or preventive activities associated with keeping the network operating including planned and unplanned maintenance. Planned maintenance is for network enhancements or action to prevent network disruptions. Unplanned maintenance is an unexpected network activity.

3.2.4.2 Network Task Group Participants

The Network Task Group assembled a diverse team of 13 individuals with representatives that include equipment suppliers, network operators, service providers and academia. In addition to members of the Task Group, subject matter experts were engaged to strengthen its expertise and develop Best Practices. Table 3.2.4.2 lists the Network Task Group participants.

Table 3.2.4.2. Network Task Group Participants.

Name	Organization
Mark Adams, ***Leader***	Cox Communications
Brent Austin	Century Telephone

Scott Bradner	Harvard University
Rick Canaday	AT&T
John Chappa	SBC
Dave Cooper	Global Crossing
Chase Cotton	Sprint
Tim Hall	ALLTEL
William Norton	Equinix
Joe Provo	RCN
Ren Provo	SBC
Brian Rooks	Qwest
Jim Runyon	Lucent Technologies-Bell Labs

3.2.4.3 Network Summary

The Network Task Group methodology was to develop Best Practices by identifying and closing gaps, identifying PDN service applicability and implementing the results of the Effectiveness Survey. The following table summarizes the results of the Best Practice work resulting from these activities. Overall, 20 new Best Practices were developed and 14 existing Best Practices were modified. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

Table 3.2.4.3. Network Task Group Summary of Best Practice Activities.

	Gap Closure Process (4 Gaps)	Effectiveness Survey Process	PDN Services Applicability Improvement Process	TOTAL
New Best Practices	15	0	5	**20**
Modified Best Practices	1	9	4	**14**
Deleted Best Practices	0	0	0	**0**

3.2.4.4 Network Gap Analysis

The Council Charter directs the Focus Group to "…*perform a gap analysis to determine areas where new Best Practices for [the Public Data Network] providers are needed*."

Initially, to encourage free form and innovative thinking the Focus Group 3B and Network Task Group used brainstorming methods and submittals by industry experts to detail a listing of 71 potential concerns for the network area of the public data network.

The 71 potential concerns were subsequently analyzed by the Network Task Group to determine if they were applicable to the public data network and potential candidates for a Best Practice. Through this analysis, the original list was consolidated into a more concise grouping of 40 potential concerns. Each potential issue on the list of 40 was analyzed in detail to determine proper disposition:

- Addressed by an existing Best Practice
- Out of Scope or not applicable to the public data network
- Consolidate with other potential Issues on the list
- Transferred to another Task Group

- Best Practice candidate

Four gaps were identified by this process:

1. Network Design and Planning
2. Network Measurement and Management
3. Network Spares Administration
4. Maintenance Window

Each of these four gaps has been closed with Best Practices by either modifying existing Best Practices or with new Best Practices. These gap closures are discussed in the following section.

3.2.4.5 Network Gap Closure

The closure of each of the four gaps identified in the previous section is described below:

1. Network Design and Planning

Analysis by the team showed that 73 Best Practices currently existed relative to network design. The Task Group then continued the analysis process and identified several opportunities to enhance NRIC Best Practices in the following areas: The treatment of design audit, routing practice and filtering. Ultimately, these gaps are proposed to be addressed with the following five new Best Practices**.**

Table 3.2.4.5.A. Network Task Group Summary of Design/Planning Gaps.

Status	BP #	Best Practice
New Practice	**7-P-0405**	**Network Performance:** Service Providers and Network Operators should periodically examine and review their network to ensure that it meets the current design specifications.
New Practice	**7-P-0408**	**Ingress Filtering:** Service Providers and Network Operators should, where feasible, implement RFC 3704 (IETF BCP84) ingress filtering.
New Practice	**7-P-0409**	**Routing Resiliency:** Service Providers should use virtual interfaces (i.e., a router loopback address) for routing protocols and network management to maintain connectivity to the network element in the presence of physical interface outages.
New Practice	**7-P-0410**	**Security Services and Procedures:** Service Providers and Network Operators should, as appropriate, review, understand, and implement "Internet Service Provider Security Services and Procedures" (RFC3013/BCP46).
New Practice	**7-P-0412**	**IP Element Security:** To enhance security, Network Operators and Service Providers should, by default, disable ICMP (Internet Control Message Protocol) redirect messages and IP source routing.

2. Network Measurement and Management

One Best Practice existed relative to Equipment Suppliers measuring and improving quality. The Task Group identified opportunities to improve the existing Best Practice by specifying applicability to Service Providers and Network Operators and expanding and clarifying the intentions of measurement/continuous improvement methodologies. This gap is proposed to be addressed with the following six new Best Practices, with one modification of an existing practice:

Table 3.2.4.5.B. Network Task Group Summary of Network Measurement Gap.

Status	BP #	Best Practice
New Practice	**7-P-0400**	**Network Performance Measurements:** Service Providers and Network Operators should establish measurements to monitor their network performance.
New Practice	**7-P-0401**	**Network Surveillance:** Service Providers and Network Operators should monitor the network to enable quick response to network issues.
New Practice	**7-P-0404**	**Network Performance:** Service Providers, Network Operators and Equipment Suppliers should incorporate methodologies that continually improve network or equipment performance.
Modify	**7-P-0518**	**Traffic Monitoring** and trending, forecasting, simulated failure analysis and emergency procedures should be designed and implemented in packet networks. Ref: NRIC VII split this BP into two parts. See BP 0616 for 'Failure Effects Analysis'
New Practice	**7-P-0616**	**Failure Effects Analysis:** Network Operators should design and implement procedures to evaluate failure and emergency conditions affecting network capacity. Ref: NRIC VII split this BP into two parts. See BP 0518 for 'Capacity Monitoring'
New Practice	**7-P-0416**	**Capacity Management:** Network Operators should design and implement procedures for traffic monitoring, trending and forecasting so that capacity management issues may be addressed.
New Practice	**7-P-0417**	**Capacity Management:** Network Operators should design and implement procedures to evaluate failure and emergency conditions affecting network capacity.

3. Network Spares Administration

At least 12 existing Best Practices touched on spare equipment. The Task Group has identified an opportunity to improve guidance in the area of spares management. This gap is proposed to be addressed with the following one new Best Practice:

Table 3.2.4.5.C. Network Task Group Summary of Network Spares Gap.

Status	BP #	Best Practice
New Practice	**7-P-0406**	**Spares and Inventory:** Service Providers and Network Operators should, where appropriate, establish a process to ensure that spares inventory is kept current to at least a minimum acceptable release (e.g., hardware, firmware or software version).

4. Maintenance Window

One current Best Practice existed for the definition of maintenance windows. The Task Group has identified opportunities to improve guidance in the communication of maintenance timeframes. This gap is proposed to be addressed with the following three new Best Practices:

Table 3.2.4.5.D. Network Task Group Summary of Maintenance Window Gap.

Status	BP #	Best Practice
New Practice	**7-P-0403**	**Maintenance Notification:** Service Providers and Network Operators should communicate maintenance windows to their customers.
New Practice	**7-P-0413**	**Maintenance Notification:** Service Providers and Network Operators should communicate information on service affecting maintenance activities and events to their customers, as appropriate.
New Practice	**7-P-0414**	**Maintenance Notification:** Service Providers and Network Operators should establish plans for internal communications regarding maintenance activities and events that impact customers.

3.2.4.6 Network Task Group Effectiveness Survey

Ten representative Best Practices were selected by the Network Task Group to be published as part of the Focus Group 3B Effectiveness Survey directed to industry users. The output from this survey was reviewed by the Network Task Group for applicability. Based on the Task Group's analysis, the following nine Best Practices are being modified:

Table 3.2.4.6. Network Task Group Summary of Effectiveness Survey Work.

Status	BP #	Best Practice
Modified Best Practice	**7-P-0515**	**Role-based Mailbox:** Network Operators and Service Providers should, for easy communication with subscribers and other operators and providers, use specific role-based accounts (e.g., abuse@provider.net, ip-request@provider.net) versus general accounts (e.g., noc@provider.net) which will help improve organizational response time and also reduce the impact of Spam.
Modified Best Practice	**7-P-0516**	**Route Flapping:** Network Operators and Service Providers should manage the volatility of route advertisements in order to maintain stable IP service and transport. Procedures and systems to manage and control route flapping at the network edge should be implemented.
Modified Best Practice	**7-P-0521**	**Industry Standards:** Network Operators, Service Providers and Equipment Suppliers should work toward implementing industry standards for interconnection points (e.g., IETF, applicable ANSI T-1 standards). Ref: The current environment of numerous Network Operators, Service Providers and Equipment Suppliers elevates the importance of standards adoption (e.g., IETF and ITU-T standards).
Modified Best Practice	**7-P-0522**	**Industry Forum Participation:** Network Operators, Service Providers, and Equipment Suppliers should participate in standards development organizations and industry forums. Ref: The current environment of numerous Network Operators, Service Providers and Equipment Suppliers elevates the importance of industry dialogue and standards (e.g., IETF, ITU-T, NANOG, NRIC).
Modified Best Practice	**7-P-0603**	**System Backup:** Network Operators and Service Providers should establish policies and procedures that outline how critical network element databases will be backed up onto a storage medium (e.g., tapes, optical diskettes) on a scheduled basis. Ref: Examples of network databases include router configurations, digital cross connect system databases, switching system images, base station controller images. These policies and procedures should address, at a minimum, the following: Database backup schedule and verification procedures; Storage medium standards; Storage medium labeling; On site and off site storage; Maintenance and certification; Handling and disposal.

Modified Best Practice	**7-P-0607**	**Inter-Provider Fault Isolation:** Network Operators and Service Providers should ensure that bilateral technical agreements between interconnecting networks address the issue of fault isolation.
Modified Best Practice	**7-P-0617**	**Route Controls:** Network Operators and Service Providers should ensure that routing controls are implemented and managed to prevent adverse routing conditions. Ref: Adverse routing conditions may include such things as infinite looping and flooding of datagrams across data networks. Controls should be implemented across network boundaries to limit the frequency of route advertisements and prevent routing of reserved or private address space. Controls should also prevent unauthorized advertisements of other operators' address space that is not legitimately allocated or assigned to the proper entity. For example, see those addressed in RFC 1918 http://www.ietf.org/rfc/rfc1918.txt.
Modified Best Practice	**7-P-0645**	**HVAC Maintenance:** Network Operators, Service Providers and Property Managers should inspect and maintain heating, venting, air conditioning (HVAC) areas.
Modified Best Practice	**7-P-5075**	**Network Diversity:** Network Operators and Service Providers should ensure that networks built with redundancy are also built with geographic separation where feasible (e.g., avoid placing mated pairs in the same location and redundant logical facilities in the same physical path).

3.2.4.7 Network Services Applicability Improvement Process

As the Network Task Team went through the detailed gap analysis and closure process, other areas not identified as gaps on the initial report emerged as potential areas for improvement. Following a review of the existing Best Practices,[17] the following five new Best Practices and four modifications to existing Best Practices were identified to improve public data network reliability:

Table 3.2.4.7. Network Services Applicability Improvement.

Status	**BP #**	**Best Practice**
New Practice	**7-P-0402**	**Single Point of Failure:** Service Providers and Network Operators should, where appropriate, design networks to minimize the impact of a single point of

[17] NRIC Best Practices web site keyword searches touching the network area resulted in the following: Reliability: 261 Procedural: 204 Network Operations: 151 Network Design: 73 Network Provisioning: 56 Technical Support: 51.

		failure.
New Practice	**7-P-0407**	**NOC Communications:** Network Operators and Service Providers should establish processes for NOC-to-NOC (Network Operations Center) peer communications for critical network activities (e.g., scheduled maintenance, upgrades and outages).
New Practice	**7-P-0411**	**Cable Management:** Network Operators and Service Providers should consider developing and implementing cable labeling standards. Reference: See Telcordia GR-1275 (Installation Standards Manual)."
New Practice	**7-P-0415**	**Data Back-up Verification:** Network Operators and Service Providers should test the restoral process associated with critical data back-up, as appropriate. The goal is to demonstrate that data restoration is complete and works as expected.
New Practice	**7-P-0418**	**Back-out MOPs:** Service Providers and Network Operators should, where appropriate, have a documented back-out plan as part of a Method of Procedure (MOP) for scheduled and unscheduled maintenance activities.
Modified Best Practice	**7-P-5196**	**MOPs:** Service Providers and Network Operators should ensure that contractors and Equipment Supplier personnel working in critical network facilities follow the current applicable MOP (Method of Procedures), which should document the level of oversight necessary.
Modified Best Practice	**7-P-0532**	**Diversity Audit:** Network Operators should periodically audit the physical and logical diversity called for by network design and take appropriate measures as needed.
Modified Best Practice	**7-P-0548**	**Post Mortem Review:** Service Providers and Network Operators should have an internal post mortem process to complete root cause analysis of major network events with follow-up implementation of corrective and preventive actions to minimize the probability of recurrence. Network Operators and Service Providers should engage Equipment Suppliers and other involved parties, as appropriate, to assist in the analysis and implementation of corrective measures.
Modified Best Practice	**7-P-8061**	**IR (Incident Response) Procedures:** Service Providers and Network Operators should establish a set of standards and procedures for dealing with computer and network security events. These procedures can and should be part of the overall business continuity/disaster recovery plan. Where possible, the procedures should be exercised periodically and revised as needed.

		Procedures should cover likely threats to those elements of the infrastructure which are critical to service delivery/business continuity. See Appendix X and Y.

3.2.4.8 Network Issues for Further Investigation

Based on scope and known processes in place, there were no issues identified by the Network Task Group that will require further investigation.

3.2.5 PAYLOAD

3.2.5.1 Payload Subject Matter

Payload includes any messages that go across networks. The payload in the public data network, typically thought of as the data associated with end-user applications, is increasingly becoming an essential element in the continued operation of our nation's communications infrastructure. Payload, whether data, image, video, or voice, is rapidly becoming a major source of communication as well as a major component of information, news, entertainment, commerce, public safety, transportation, national security, and emergency response.

Payload in the sense of the public data network most commonly refers to the data contained inside the IP packet within the TCP/IP protocol suite. The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another across any IP enabled network, although we will generically use Internet within this report. When an end-user's application sends or receives data (e.g., an e-mail note or a Web page), the message gets divided into little chunks of data called packets. Each of these packets of data also contains both the sender's Internet address and the receiver's address. Packets are sent first to a router that understands a small part of the Internet then are passed onto subsequent routers until the packet reaches the destination.

Unlike circuit switch networks, IP is a connectionless protocol, which means that there is no fixed path or continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. The most widely used version of IP today is Internet Protocol Version 4 (IPv4). However, IP Version 6 (IPv6) is also beginning to be supported.

3.2.5.2 Payload Task Group Participants

The Payload Task Group assembled a team of sufficient expertise to effectively address the payload subject matter as it relates to the reliability of the public data network. The Payload Task Group was made up of six participants. In addition to members of the Focus Group, the Task Group engaged other subject matter experts to strengthen its expertise. Table 3.2.5.2 lists the Payload Task Group participants. The team had sufficient expertise to complete this activity.

Table 3.2.5.2. Payload Task Group Participants.

Name	Organization
Solos Arthachinda	IBasis
Ajay Joseph	IBasis
David Frigeri, ***Leader***	Internap Network Services
Manny Sidhu	Internap Network Services
Jon Vestal	Internap Network Services
Jim Runyon	Lucent Technologies, Bell Labs

3.2.5.3 Payload Summary of Best Practice Activities

The Payload Task Group methodology was to develop Best Practices by identifying and closing gaps, identifying PDN service applicability and implementing the results of the Effectiveness Survey. The following table summarizes the results of the Best Practice work resulting from these activities. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

Table 3.2.5.3. Payload Task Group Summary of Best Practice Activities.

	Gap Closure Process (0 Gaps)	Effectiveness Survey Process	PDN Services Applicability Improvement Process	TOTAL
New Best Practices	0	0	1	**1**
Modified Best Practices	0	0	0	**0**
Deleted Best Practices	0	0	0	**0**

3.2.5.4 Payload Gap Analysis

The Council Charter directs the Focus Group to *"…perform a gap analysis to determine areas where new Best Practices for [the Public Data Network] providers are needed."* As described in Section 2.3.5, the approach used for payload was similar for the other areas. Therefore, a gap is here defined as a space between the known problems associated with payload that can impact network reliability and the existing Best Practices for payload. To understand the former boundary, a list was generated of 30 known concerns for payload. To understand the latter boundary, the existing Best Practices were researched and 48 were found to have potential application to public data network reliability.[18] In addition, the Payload Task Group reviewed the work of the previous Council in which the vulnerabilities of payload were systematically reviewed.[19] [20]

3.2.5.5 Payload Gap Closure

The Task Group's gap analysis determined that there were no significant gaps in the payload area.

[18] The NRIC Best Practices related to bandwidth monitoring were 6-6-8074 and 6-6-8075. The NRIC Best Practices identified using the keyword "signaling" were 6-5-0517, 6-6-8040, 6-6-0770, 6-6-8040, 6-6-8051, 6-6-8052, 6-6-8053, 6-6-8054, 6-6-8060 and 6-6-8104. The NRIC Best Practices identified using the keyword "encryption" were 6-6-5062, 6-6-8001, 6-6-8006, 6-6-8012, 6-6-8013, 6-6-8025, 6-6-8028, 6-6-8029, 6-6-8049, 6-6-8051, 6-6-8052, 6-6-8059, 6-6-8060, 6-6-8091, 6-6-8094, 6-6-8096, 6-6-8105 and 6-6-8503. The search string "interception" resulted in 6-6-5173. For bandwidth variations (e.g., Mass calling), Best Practices 6-6-0576, 6-6-8074 and 6-6-8075 were identified.

[19] The Homeland Security Physical Security Focus Group (1A) of NRIC VI carefully listed the *categories* of payload vulnerability. See NRIC VI Homeland Security Physical Security Focus Group Final Report, Issue, 3, December 2003, p. 49.

[20] Network Reliability and Interoperability Council Homeland Defense, Focus Group 1B (Cyber Security): Summary Report and Proposals from Cyber Security Best Practices Work Completed by FG1B Between March 2002 and March 2003.

3.2.5.6 Payload Effectiveness Survey Process

The payload Best Practices selected for the Effectiveness Survey were rated effective or moderately effective and, as such, no modifications were identified.

3.2.5.7 Payload Services Applicability Improvement Process

The Council Charter directs the Focus Group to *"…focus on the special needs of public data services providers and refine existing Best Practices to improve their applicability to Internet data services and other public data network services*." As described in Section 2.1, the Payload Task Group was assigned a number of areas of concern. Each concern was systematically investigated to determine if an existing Best Practice already addressed the concern, if an existing Best Practice needed to be modified to adequately address the concern, or if a new Best Practice needed to be created. Based on this analysis, one new Best Practice was developed.

- **7-P-0442 Network Measurement:** Service Providers should consider measuring end-to-end path performance and path validity for both active and alternate routes.

3.2.5.8 Payload Issues for Further Investigation

Based on scope and known processes in place, there were no issues identified by the Payload Task Group that will require further investigation.

3.2.6 POLICY

3.2.6.1 Policy Subject Matter

The policy area includes agreements between multiple parties covering issues such as industry standards and practices, along with physical and logical interfaces (e.g., protocols). The Internet, like many other data networks, is formed of many networks owned and operated independently by a large number of network operators. Continued success in providing a high reliability service offering over a network formed of multiple administrative domains clearly depends upon industry agreement on operating methods, procedures, and common protocol suites.

Practices associated with the policy area have a critical role in the reliability of the public data network. Increasingly this focus is associated with the Internet. The transport of an end customer's Internet Protocol (IP) datagrams across the Internet (commonly called IP "transit") depends upon both the family of IP protocol standards and a common industry framework of how addressing and routing should happen.

The Policy Task Group considered the following areas specifically related to the public data network and Internet service providers to identify policy related issues:

IP Addressing: Mechanisms for management of a provider's IP addresses and address spaces.

Naming (DNS): Mechanisms associated with the Domain Name System (DNS) and the mapping between IP addresses and domain names.

Routing: Mechanisms for maintaining a provider's network topology and distribution of prefixes (routes) internally.

Interconnection: Mechanisms for exchanging routes between providers.

Abuse: Mechanisms for dealing with network abuse (DOS, Spam, etc.).

The Policy Task Group believes this taxonomy broadly covers the current practice space associated with design, engineering, and operations in the modern public data network. The Policy Task Group also considered several additional practice areas, not specifically related to Internet Service Providers, but having general application to all public data network operators:

Network Management: Mechanisms for element and overall network management, provisioning, and surveillance.

Service Assurance (sometimes called Service Delivery): Ongoing management of customer's services.

Provider-Customer: Interactions and mechanisms between a provider and a customer.

Inter-Provider: Interactions and mechanisms between two providers.

This review revealed that the existing NRIC Best Practices covered specific issues quite thoroughly (e.g., BGP filtering) but did not always address many common industry accepted practices (e.g., use of Classless Inter-Domain Routing, CIDR). These issues were reviewed by the Policy and Network Task Groups.

3.2.6.2 Policy Task Group Participants

The Policy Task Group assembled a team of sufficient expertise to effectively address the policy subject matter as it relates to the reliability of Internet service providers and the public data network. The Policy Task Group was made up of ten participants with representatives that included equipment suppliers, network operators and service providers. In addition to members of the Focus Group, the Task Group engaged other subject matter experts to strengthen its expertise and develop proposed Best Practices. The primary disciplines of network architecture, design, engineering, operations, standards, measurement, and testing were represented on the team. Care was also taken to include representation from a broad range of industry roles. Table 3.2.6.2 lists the Policy Task Group participants.

Table 3.2.6.2. Policy Task Group Participants.

Name	Organization
Mark Adams	Cox Communications
Scott Bradner	Harvard University
Dean Brewster	Comcast
Rick Canaday	AT&T
Chase Cotton, ***Leader***	Sprint
William Norton	Equinix
Joe Provo	RCN
Ren Provo	SBC
Brian Rooks	Qwest
Jim Runyon	Lucent Technologies-Bell Labs

3.2.6.3 Policy Summary

The Policy Task Group methodology was to develop Best Practices by identifying and closing gaps, identifying PDN service applicability and implementing the results of the Effectiveness Survey. The following table summarizes the results of the Best Practices resulting from these activities. Overall, five new Best Practices were developed. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

Table 3.2.1.3. Policy Task Group Summary of Best Practice Activities.

	Gap Closure Process (1 Gap)	Effectiveness Survey Process	PDN Services Applicability Improvement Process	TOTAL
New Best Practices	0	0	5	**5**
Modified Best Practices	0	0	0	**0**
Deleted Best Practices	0	0	0	**0**

3.2.6.4 Policy Gap Analysis

The Council Charter directs the Focus Group to "…*perform a gap analysis to determine areas where new Best Practices for [the Public Data Network] providers are needed*." A gap is defined as a space between the known problems associated with the policy area that can impact network reliability and the existing Best Practices for policy.

To encourage free form and innovative thinking, the Focus Group and Policy Task Group used brainstorming and analysis methods or submittals by industry experts to detail a listing of 65 potential concerns for the policy area of the public data network. The 65 potential concerns were subsequently analyzed by the Policy Task Group to determine if they were applicable to the public data network and potential candidates for Best Practices.

The Policy Task Group also surveyed existing Best Practices in possible policy areas and other common industry practices and keywords and found reasonable coverage of Internet service provider topics:

Internet	27[21]
IP (Internet Protocol)	20[22]
routing	33[23] (not all IP specific)
peering	10[24]
CIDR (Classless Inter-Domain Routing)	1[25]
domain, DNS (Domain Name System)	8[26], 13[27]
BGP (Border Gateway Protocol)	6[28]
service assurance	2[29]
inter-provider	0
SLA (Service Level Agreement)	4[30]
QoS (Quality of Service)	2[31]
ISP (Internet Service Provider)	16[32]

[21] see NRIC Best Practices 6-5-0506, 6-5-0508, 6-5-0608, 6-6-3210, 6-6-5068, 6-6-8008, 6-6-8015, 6-6-8029, 6-6-8043, 6-6-8046, 6-6-8047, 6-6-8048, 6-6-8051, 6-6-8052, 6-6-8068, 6-6-8070, 6-6-8077, 6-6-8079, 6-6-8080, 6-6-8081, 6-6-8083, 6-6-8086, 6-6-8090, 6-6-8093, 6-6-8525, 6-6-8527, 6-6-8528

[22] see NRIC Best Practices 6-5-0506, 6-5-0507, 6-5-0508, 6-5-0516, 6-5-0533, 6-6-0762, 6-6-0764, 6-6-0765, 6-6-0769, 6-6-8040, 6-6-8043, 6-6-8051, 6-6-8055, 6-6-8056, 6-6-8057, 6-6-8090, 6-6-8106, 6-6-8522, 6-6-8535, 6-6-8539

[23] see NRIC Best Practices 6-5-0500, 6-5-0510, 6-5-0516, 6-5-0519, 6-5-0520, 6-5-0524, 6-5-0526, 6-5-0566, 6-5-0568, 6-5-0570, 6-5-0572, 6-5-0579, 6-5-0603, 6-5-0617, 6-5-0618, 6-5-0622, 6-5-0651, 6-5-0679, 6-5-0709, 6-5-0727, 6-5-0731, 6-6-5107, 6-6-8041, 6-6-8042, 6-6-8043, 6-6-8045, 6-6-8049, 6-6-8050, 6-6-8108, 6-6-8525, 6-6-8526, 6-6-8531, 6-6-8565

[24] see NRIC Best Practices 6-5-0503, 6-5-0524, 6-6-0806, 6-6-8040, 6-6-8042, 6-6-8043, 6-6-8044, 6-6-8050, 6-6-8093, 6-6-8525

[25] see NRIC Best Practices 6-5-0503

[26] see NRIC Best Practices 6-5-0510, 6-6-8015, 6-6-8046, 6-6-8047, 6-6-8048, 6-6-8089, 6-6-8527, 6-6-8528

[27] see NRIC Best Practices 6-5-0510, 6-5-0523, 6-6-0762, 6-6-0763, 6-6-8042, 6-6-8043, 6-6-8044, 6-6-8046, 6-6-8047, 6-6-8048, 6-6-8525, 6-6-8527, 6-6-8528

[28] see NRIC Best Practices 6-5-0516, 6-6-8042, 6-6-8043, 6-6-8044, 6-6-8050, 6-6-8525

[29] see NRIC Best Practices 6-5-0530, 6-5-0547

[30] see NRIC Best Practices 6-6-0802, 6-6-0811, 6-6-8504, 6-6-8506

[31] see NRIC Best Practices 6-5-0521, 6-6-0811

• RFC (Request For Comments)	16[33]
• AUP (Acceptable Use Policy)	4[34]
• Spam	1[35]
• DOS (Denial of Service)	12[36] (not all Internet specific)

3.2.6.5 Policy Gap Closure

The Policy Task Group's gap analysis determined that there were no significant gaps in the policy area from an industry practice standpoint. The Policy Task Group's gap analysis did however determine that there were some common best industry practices that are not adequately covered in the existing NRIC Best Practices (see Section 3.2.6.7).

3.2.6.6 Policy Effectiveness Survey Process

The Policy Best Practices selected for the Effectiveness Survey were rated effective and, as such, no modifications were identified.

3.2.6.7 Policy Services Applicability Improvement Process

Per the NRIC VII charter, the PDN Focus Group was to *"…refine existing Best Practices to improve their applicability to Internet data services and other public data network services."* New Best Practices proposed for the policy area are shown in Table 3.2.6.7.

Table 3.2.6.7. Policy Task Group New Best Practices Summary.

Status	BP #	Best Practice
New Practice	**7-P-0437**	**Route Aggregation:** Network Operators and Service Providers should aggregate routes where appropriate (e.g., singly-homed downstream networks) in order to minimize the size of the global routing table.
New Practice	**7-P-0438**	**CIDR Use:** Network Operators and Service Providers should enable CIDR (Classless Inter-Domain Routing) by implementing classless route prefixes on routing elements.
New Practice	**7-P-0439**	**BGP Authentication:** Network Operators and Service Providers should authenticate BGP sessions (e.g., using TCP MD5) with their own customers and other providers.
New Practice	**7-P-0440**	**Route Exchange Limits:** Network Operators and Service Providers should set and periodically review situation-specific limits on numbers of routes imported from peers and customers in order to lessen the impact of misconfigurations.

[32] see NRIC Best Practices 6-5-0502, 6-6-5068, 6-6-8042, 6-6-8043, 6-6-8044, 6-6-8050, 6-6-8066, 6-6-8078, 6-6-8079, 6-6-8080, 6-6-8092, 6-6-8093, 6-6-8513, 6-6-8514, 6-6-8525, 6-6-8531

[33] see NRIC Best Practices 6-5-0515, 6-5-0516, 6-5-0617, 6-6-0763, 6-6-0764, 6-6-0765, 6-6-0767, 6-6-0768, 6-6-8046, 6-6-8047, 6-6-8048, 6-6-8050, 6-6-8070, 6-6-8527, 6-6-8528, 6-6-8531

[34] see NRIC Best Practices 6-5-0533, 6-6-8092, 6-6-8514, 6-6-8521

[35] see NRIC Best Practice 6-5-0533

[36] see NRIC Best Practices 6-5-0506, 6-5-0533, 6-6-8043, 6-6-8053, 6-6-8074, 6-6-8075, 6-6-8076, 6-6-8523, 6-6-8528, 6-6-8530, 6-6-8533, 6-6-8561

New Practice	**7-P-0441**	**Unicast RPF:** Network Operators and Service Providers should, where feasible, implement Unicast RPF (Reverse Path Forwarding) to help minimize DOS attacks that use source address spoofing.

3.2.6.8 Policy Issues for Further Investigation

Based on scope and known processes in place, there are, for the policy area, no items identified for further investigation.

3.2.7 POWER

3.2.7.1 Power Subject Matter

The Power area includes the internal power systems, batteries, grounding, high voltage and other cabling, fuses, back-up emergency generators and fuel.[37] Power is an essential basic element of the communications infrastructure, without which networks will not function. In addition, any power problem has the potential to become a catastrophe, potentially damaging other equipment and personnel.[38]

3.2.7.2 Power Task Group Participants

The Power Task Group assembled a team of experts to effectively address the Power subject matter as it relates to the reliability of the public data network. The Power Task Group was made up of seven participants. Network operators, power equipment manufactures, telecommunications equipment suppliers and academia were all represented on the team. In addition, the Task Group engaged other subject matter experts to strengthen its expertise. Table 3.2.7.2 lists the Power Task Group participants. The team had the requisite expertise to complete this activity.

Table 3.2.7.2. Power Group Task Group Participants.

Name	Organization
Scott Bradner	Harvard University
Dean Brewster	Comcast Communications
Chase Cotton	Sprint
Ray Cruz	Internap Network Services
Rick Krock, ***Leader***	Lucent Technologies-Bell Labs
Jim Runyon	Lucent Technologies-Bell Labs
Howard Washer	BatteryCorp

3.2.7.3 Power Summary

The Power Task Group methodology was to develop Best Practices by identifying and closing gaps, identifying PDN service applicability and implementing the results of the Effectiveness Survey. The following table summarizes the results of the Best Practices resulting from these activities. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

[37] The communications infrastructure is also dependent on commercial energy. This commercial power is external to the communications infrastructure.

[38] NRIC VI Homeland Security Physical Security Focus Group Final Report, Issue, 3, December 2003, p. 44

Table 3.2.7.3. Power Task Group Summary of Best Practice Activities.

	Gap Closure Process (2 Gap)	Effectiveness Survey Process	PDN Services Applicability Improvement Process	TOTAL
New Best Practices	0	0	0	**0**
Modified Best Practices	1	0	0	**1**
Deleted Best Practices	0	0	0	**0**
Recommendations	1	0	0	**1**

3.2.7.4 Power Gap Analysis

The Council Charter directs the Focus Group to *"… perform a gap analysis to determine areas where new Best Practices for [the Public Data Network] providers are needed."* As described in Section 2.3.5, the approach used by the Power Task Group was similar for the other areas. Therefore, a gap is here defined as a space between the known problems associated with power that can impact the public data network reliability and the existing Best Practices for power. To understand the former boundary, a list of ten concerns related specifically to power in the public data network was generated. To understand the latter boundary, the existing NRIC VI Best Practices pertaining to power (approximately 100[39]) were researched. The concerns were identified as being adequately addressed by existing Best Practices, transferred to the Network Task Group, or identified as gaps. The Task Group identified two gaps. One gap dealt with proper identification of cables, and the other dealt with back-up power for on-premise emerging data services equipment.

3.2.7.5 Power Gap Closure

Proper Identification of Cables

Administration, maintenance and operations of network elements depend on proper identification of equipment. While there are numerous Best Practices that address administration, operations and maintenance, and while network operators currently employ various effective methods of cable labeling, the NRIC Best Practices do not document guidance in this area. This gap was transferred to the Network Task Group, and they proposed a new Best Practice (BP 7-P-0411).

[39] 6-6-0512, 6-5-0527, 6-5-0543, 6-5-0544, 6-5-0622, 6-5-0623, 6-5-0624, 6-5-0625, 6-5-0627, 6-5-0634, 6-5-0635, 6-5-0636, 6-5-0637, 6-5-0638, 6-5-0642, 6-5-0644, 6-5-0648, 6-5-0650, 6-5-0651, 6-5-0652, 6-5-0653, 6-5-0654, 6-6-0655, 6-5-0656, 6-5-0657, 6-5-0658, 6-5-0659, 6-5-0660, 6-5-0661, 6-5-0662, 6-5-0663, 6-5-0664, 6-5-0665, 6-5-0666, 6-5-0667, 6-5-0668, 6-5-0669, 6-5-0670, 6-5-0671, 6-5-0672, 6-5-0673, 6-5-0674, 6-5-0675, 6-5-0676, 6-5-0677, 6-5-0678, 6-5-0679, 6-5-0680, 6-5-0681, 6-5-0682, 6-5-0683, 6-5-0684, 6-5-0685, 6-5-0687, 6-5-0688, 6-5-0689, 6-5-0690, 6-5-0691, 6-5-0692, 6-5-0693, 6-5-0694, 6-5-0695, 6-5-0696, 6-5-0697, 6-5-0698, 6-5-0699, 6-5-0700, 6-5-0701, 6-5-0702, 6-5-0703, 6-6-0760, 6-6-0761, 6-6-1027, 6-6-1028, 6-6-1029, 6-6-1030, 6-6-1067, 6-6-5041, 6-6-5042, 6-6-5058, 6-6-5073, 6-6-5076, 6-6-5197, 6-6-5203, 6-6-5204, 6-6-5205, 6-6-5206, 6-6-5207, 6-6-5208, 6-6-5209, 6-6-5210, 6-6-5211, 6-6-5212, 6-6-5213, 6-6-5214, 6-6-5216, 6-6-5231, 6-6-5232, 6-6-5241, 6-6-5275, 6-P-5281

Back-Up Power for On-Premise Emerging Data Services Equipment

Emerging data services, such as Voice over IP (VoIP) are increasingly viewed as critical services. As such, this equipment may need to continue to function even during commercial power outages. Because the end user equipment is increasingly powered by local sources, back-up power consideration should be explored. As these networks are still very new, further analysis is pending. A modification to an existing Best Practice will partially address this gap.

- **7-P-5058 Back-up Power:** Service Providers, Network Operators, Equipment Suppliers and Property Managers should ensure that all critical infrastructure facilities, including the security equipment, devices and appliances protecting it, are supported by backup power systems (e.g., batteries, generators, fuel cells).

3.2.7.6 Power Effectiveness Survey Process

The power Best Practices selected for the Effectiveness Survey were rated effective or moderately effective and, as such, no modifications were identified.

3.2.7.7 Power Services Applicability Improvement Process

Per the NRIC VII charter, the PDN Focus Group was to *"…refine existing Best Practices to improve their applicability to Internet data services and other public data network services."*

The Task Group was assigned issues of concern, some of which were identified as gaps in existing Best Practices (see Section 3.2.7.4). Other issues required actions to be taken to create new or modify existing Best Practices. For the Power Task Group, all the identified issues were addressed by existing Best Practices.

3.2.7.8 Power Issues for Further Investigation

Based on scope, there are some issues that will require further investigation. For the power area, there was one item identified for further investigation relating to the issue of back-up power for on-premise emerging data services equipment. The Power Task Group is providing the following recommendation:

> The issue of power for residential and business premises equipment may need to be considered, primarily as it relates to access to essential services during commercial power outages. Cordless wireline phones require electrical power to operate, and wireless phones are limited to the life of the handset battery. The spread of alternate technologies (e.g., VoIP) as a primary communications service expands this issue. Focus Group 3B has identified this issue as something that may need attention, but is outside the area of its charter.

3.2.8 SOFTWARE

3.2.8.1 Software Subject Matter

Software has a critical role in the reliability of the public data network. The software area includes the broad category of operating systems, applications, and firmware that are part of a communications system. Software spans switches, routers, transport equipment, transmission equipment, access equipment, satellites, dishes, undersea cables, microwave repeaters, cell sites, PCs, and end user devices. There are thousands of routers and switches from several different equipment suppliers deployed in United States public networks, many of which employ Software Defined Networks (SDNs) such as Virtual Private Networks (VPNs). The number of lines of code in the communications networks in the United States is in the hundreds of millions. Both network and systems engineers rely heavily on network management software and software services to operate and maintain their networks. Despite the diversity of hardware in use in the public networks, there is a wide variety of agreed upon software standards available, and in use, that allow interoperability and manageability.

3.2.8.2 Software Task Group Participants

The Software Task Group assembled a team of sufficient expertise to effectively address the software subject matter as it relates to the reliability of the public data network. The Software Task Group consisted of nine participants. In addition to members of the Focus Group, the Task Group engaged other subject matter experts to strengthen its expertise. The primary software disciplines were present on the team. Table 3.2.8.2 lists the Software Task Group participants. Included was representation from a broad range of industry roles and varying technologies. The team had sufficient expertise to complete this activity.

Table 3.2.8.2. Software Task Group Participants.

Name	Organization
Robin Roberts	Cisco Systems
Jon Vestal	Internap Network Services
Duke McMillan	Internap Network Services
Jim Fliers	Internap Network Services
Fred Stringer	Juniper Networks
Paul Wolfson	Lucent Technologies
Art Morrical	Lucent Technologies
Brad Nelson, ***Leader***	Quality & Reliability Solutions, LLC
Jim Runyon	Lucent Technologies-Bell Labs

3.2.8.3 Software Summary

The Software Task Group methodology was to develop Best Practices by identifying and closing gaps, documenting dependencies, identifying PDN service applicability, and implementing the results of the Effectiveness Survey. The following table summarizes the results of the Best Practices resulting from these activities. Subsequent sub-sections will provide additional details for each of the activities defined in the methodology.

Table 3.2.8.3. Software Task Group Summary of Best Practice Activities.

	Gap Closure Process (4 Gaps)	Effectiveness Survey Process	PDN Services Applicability Improvement Process	TOTAL
New Best Practices	9	0	0	**9**
Modified Best Practices	0	0	0	**0**
Deleted Best Practices	0	0	0	**0**

3.2.8.4 Software Gap Analysis

The Council Charter directs the Focus Group to "…*perform a gap analysis to determine areas where new Best Practices for [the Public Data Network] providers are needed*." The approach used for software was similar for the other areas. Therefore, a gap is here defined as a space between the problems associated with software that impact network reliability and the existing Best Practices for software.

To understand the former boundary, the Task Group generated a list of 42 concerns. Upon further review and comparison to 216 existing NRIC Best Practices,[40] the Task Group identified four (4) gaps spanning the following areas:

[40] 6-5-0500, 6-5-0506, 6-5-0507, 6-5-0523, 6-5-0533, 6-5-0535, 6-5-0536, 6-5-0537, 6-5-0538, 6-5-0541, 6-5-0550, 6-5-0551, 6-5-0552, 6-5-0553, 6-5-0554, 6-5-0555, 6-5-0557, 6-5-0559, 6-5-0585, 6-5-0590, 6-5-0600, 6-5-0601, 6-5-0749, 6-5-0750, 6-6-0762, 6-6-0763, 6-6-0764, 6-6-0765, 6-6-0766, 6-6-0767, 6-6-0768, 6-6-0769, 6-6-0770, 6-6-0802, 6-6-0806, 6-6-0807, 6-6-0808, 6-6-0809, 6-6-0811, 6-6-0813, 6-6-1003, 6-6-1005, 6-6-5061, 6-6-5084, 6-6-5121, 6-6-5142, 6-6-5165, 6-6-5167, 6-6-5172, 6-6-5200, 6-6-5218, 6-6-5219, 6-6-5254, 6-6-5276, 6-6-5277, 6-6-5278, 6-6-5279, 6-6-8000, 6-6-8001, 6-6-8002, 6-6-8003, 6-6-8004, 6-6-8005, 6-6-8006, 6-6-8007, 6-6-8008, 6-6-8009, 6-6-8010, 6-6-8011, 6-6-8012, 6-6-8013, 6-6-8014, 6-6-8015, 6-6-8016, 6-6-8017, 6-6-8018, 6-6-8019, 6-6-8020, 6-6-8021, 6-6-8022, 6-6-8023, 6-6-8024, 6-6-8025, 6-6-8026, 6-6-8027, 6-6-8028, 6-6-8029, 6-6-8030, 6-6-8031, 6-6-8032, 6-6-8033, 6-6-8034, 6-6-8035, 6-6-8036, 6-6-8037, 6-6-8038, 6-6-8039, 6-6-8040, 6-6-8041, 6-6-8042, 6-6-8043, 6-6-8044, 6-6-8045, 6-6-8046, 6-6-8047, 6-6-8048, 6-6-8049, 6-6-8050, 6-6-8051, 6-6-8052, 6-6-8053, 6-6-8054, 6-6-8055, 6-6-8056, 6-6-8057, 6-6-8058, 6-6-8059, 6-6-8060, 6-6-8061, 6-6-8062, 6-6-8063, 6-6-8064, 6-6-8065, 6-6-8066, 6-6-8067, 6-6-8068, 6-6-8069, 6-6-8070, 6-6-8071, 6-6-8072, 6-6-8073, 6-6-8074, 6-6-8075, 6-6-8076, 6-6-8077, 6-6-8078, 6-6-8079, 6-6-8080, 6-6-8081, 6-6-8082, 6-6-8083, 6-6-8084, 6-6-8085, 6-6-8086, 6-6-8087, 6-6-8088, 6-6-8089, 6-6-8090, 6-6-8091, 6-6-8092, 6-6-8093, 6-6-8094, 6-6-8095, 6-6-8096, 6-6-8097, 6-6-8098, 6-6-8099, 6-6-8100, 6-6-8101, 6-6-8102, 6-6-8103, 6-6-8104, 6-6-8105, 6-6-8106, 6-6-8108, 6-6-8109, 6-6-8110, 6-6-8500, 6-6-8501, 6-6-8502, 6-6-8503, 6-6-8504, 6-6-8505, 6-6-8506, 6-6-8507, 6-6-8508, 6-6-8509, 6-6-8510, 6-6-8513, 6-6-8514, 6-6-8515, 6-6-8517, 6-6-8519, 6-6-8521, 6-6-8522, 6-6-8523, 6-6-8525, 6-6-8526, 6-6-8527, 6-6-8528, 6-6-8530, 6-6-8531, 6-6-8532, 6-6-8533, 6-6-8534, 6-6-8535, 6-6-8537, 6-6-8539, 6-6-8540, 6-6-8548, 6-6-8549, 6-6-8551, 6-6-8553, 6-6-8554, 6-6-8555, 6-6-8556, 6-6-8557, 6-6-8559, 6-6-8561, 6-6-8562, 6-6-8563, 6-6-8564, 6-6-8565, 6-6-8566, 6-6-8567

- **Management Information Base (MIB)**[41]
  Due to the quantity and interactions of "private" MIB extensions with proprietary and other management software, the Task Group identified opportunities to enhance NRIC Best Practices in the areas of MIB support, standardization, and documentation. In addition, opportunities to improve support of environmental variables in MIBs were identified.

- **Crash Diagnostic Memory**
  The Task Group identified opportunities to enhance NRIC Best Practices in the area of crash diagnostic memory storage and the use of non-volatile memory and to improve storage of core dumps and system states associated with a crash.

- **Software Configuration**
  The Task Group identified opportunities to enhance NRIC Best Practices in the area of software configuration change management and version control. Opportunities to make improvements in the following areas were identified.
  - change management documentation, revision change history, and source material
  - guidance in the area of software production standards affecting software configurations and software back-ups
  - enhancements to Best Practices in the area of manual and automated software configurations affecting installation and back-out procedures, change tools, upgrades, and limited/phased deployments.

- **Test Environment Descriptions and Published Capacity**
  The Task Group identified opportunities to enhance NRIC Best Practices in the area of test environment descriptions along with the use of "published" capacity in software testing and qualification.

3.2.8.5 Software Gap Closure

The following ten new NRIC Best Practices have been defined to address the gaps that were identified by the Software Task Group.

Management Information Base (MIB) Gap Closure
Two Best Practices were developed to close the Management Information Base (MIB) Gap.

- **7-P-0432 Standardized MIBs:** Equipment Suppliers should support standardized MIBs (Management Information Bases) and maintain documentation of private and enterprise MIBs.

[41] A MIB is a database of managed objects accessed by network management protocols. It is a hierarchical collection of objects organized in a tree. To prevent naming conflicts, the Internet Assigned Numbers Authority (IANA) manages the structure and objects in the tree. While the top levels of the MIB are fixed, the IETF, equipment manufacturers, vendors and other organizations have defined specified sub-trees. Many managed devices also have "private" MIB extensions. These extensions make it possible to report additional information to a particular equipment manufacturer's proprietary management software or to other management software that is aware of the "private" MIB extensions. In 2005, the website "mibDepot" claimed that it indexes over 6,200 MIBs representing more than 910,000 MIB object definitions.

> **Reference:** Enterprise MIBs are those written by vendors for their particular object. The managed object can furnish both standard MIB and enterprise MIB information. The standard MIBs are those that have been approved by the IAB (Internet Architecture Board, www.iab.org). Equipment and software vendors define the private MIBs unilaterally.

- **7-P-0433 MIB Environment Variables:** Equipment Suppliers should support, clearly define and document environmental variables in Management Information Bases (MIB).

  > **Reference:** MIB Environmental variables include the location of hosts, servers, terminals and other nodes as well as the traffic for the object.

Crash Diagnostic Memory Gap Closure
One Best Practice was developed to close the Crash Diagnostic Memory Gap.

- **7-P-0429 Crash Diagnostics:** Equipment Suppliers should provide appropriate storage and retrieval mechanisms for diagnostics after a hardware or software crash.

  > **Reference:** Information useful for diagnostics might include core dumps and register contents.

Software Configuration Gap Closure
Five Best Practices were developed to close the Crash Diagnostic Memory Gap.

- **7-P-0425 Software Management:** Service Providers and Network Operators should maintain software version deployment records, as appropriate.

- **7-P-0426 Software Change Control:** Equipment Suppliers should use software change control to manage changes to source material used in the production of their products.

  > **Reference:** As such, the software change control system used by equipment suppliers should be able to manage both ASCII and binary (source object code) files.

- **7-P-0427 Software Documentation:** Equipment Suppliers should maintain software documentation including revision change history and associated release notes.

- **7-P-0428 Software & Hardware Vulnerability Tracking:** Service Providers should monitor software and hardware vulnerability reports and take the recommended action(s) to address problems, where appropriate. These reports and recommendations are typically provided by equipment suppliers and CERTs (Computer Emergency Response Teams).

7-P-0430 Software Configurations: Equipment Suppliers should be able to recreate supported software from source and, where feasible, software obtained from third parties.

Test Environment Descriptions and Published Capacity Gap Closure
One Best Practice was developed to close the Test Environment Descriptions and Published Capacity Gap.

7-P-0431 Capacity and Performance Data: Equipment Suppliers should provide capacity and performance data for network elements.

Reference: Use commonly agreed upon terminologies and methodologies such as those developed by IETF Benchmarking Methodology Working Group (e.g., RFC 2544).

3.2.8.6 Software Effectiveness Survey Process

The Software Best Practices selected for the Effectiveness Survey were rated effective or moderately effective and, as such, no modifications were identified.

3.2.8.7 Software Services Applicability Improvement Process

The Software Task Group found that, except for the gaps identified above, the existing software Best Practices adequately addressed the software issues for the public data network.

3.2.8.8 Software Issues for Further Investigation

Based on scope and known processes in place, there are no software issues that have be identified for further investigation.

3.3 Survey of Effectiveness

This section describes how the focus group fulfilled the requirement in its mission to conduct an industry survey on the effectiveness of existing Best Practices. Specifically, the NRIC VII Charter directs the Council to *"… survey providers of public data network services, including Internet data services providers, concerning the efficacy of existing Best Practices."* The Charter further directs that "By April 29, 2005, the Council shall complete its survey of the effectiveness of the Best Practices for Internet data services."

3.3.1 Additional Industry Engagement

Getting an outside perspective is one of the principles of developing Best Practices.[42] Conducting industry surveys of Best Practices has been part of several previous Councils. While NRIC Focus Groups typically have broad representation, these surveys usually extend to even a wider reach. For example, some companies may not have the resources to participate in the monthly meetings. However, the survey is a way for their perspective to be included in the process.

3.3.2 Use of Third Party

Because information collected on Best Practices from an individual company may be sensitive, the Focus Group elected to employ a trusted, third party entity to assist in conducting the survey. With the guidance of the Charter, the Focus Group prioritized the following criteria in its Request for Proposal (RFP) process:

- Approach to supplying the services sought
- Demonstrated organizational capability
- Qualifications of personnel
- Price

Since the Wireless Network Reliability Focus Group (3A), had a similar survey requirement in its mission, the selection process was coordinated across the two Focus Groups. The joint Focus Group evaluation process resulted in the selection of BPI-Telcodata[43] to conduct this industry survey.

3.3.3 Timeline

The survey was completed between December, 2004 and March, 2005. The larger timeline can be summarized as follows:

- December 2004 – charter interpretation, RFP development, RFP outreach, RFP response analysis
- January 2005 – field test, commencement of survey
- February 2005 – completion of survey
- March 2005 – analysis of results
- April – June 2005 – Best Practice adjustments based on learnings

[42] Section 2.3.2, Principle 6

[43] BPI-Telcodata is an independent consulting firm that provides benchmarking and best practice consulting, regulatory support, demand analysis and forecasting, survey and database services for carriers and vendors on many areas including service reliability, cost analysis, market planning and other performance metrics. www.telcodata.net

3.3.4 Approach

There are hundreds of Best Practices that apply to the reliability of the Public Data Network. In order to have a survey that respondents could complete in a reasonable amount of time, the number of Best Practices could not be too large. Therefore the Focus Group selected representative Best Practices from each of the eight communications infrastructure ingredients: Environment, Hardware, Human, Network, Payload, Policy, Power and Software. The respective Task Group leaders and subject matter experts selected ten Best Practices that best represented these areas. The number of Best Practices selected represented approximately a quarter of those applicable.

This survey was designed to catalog and analyze the opinions of service providers, network operators and equipment suppliers regarding the effectiveness of Best Practices. Four questionnaires were fielded, two for service providers and network operators (Wireless and Public Data Network) and two for equipment suppliers (Wireless and Public Data Network).[44] The respondents rated the effectiveness of each Best Practice on network reliability.[45] Respondents were also given the opportunity to provide comments and other feedback on each Best Practice.

BPI-Telcodata designed and distributed the questionnaires, collected and tabulated the responses, and produced detailed reports with tables, graphs and respondent commentaries. All of the responses were treated as proprietary information and careful security measures were used to ensure that, whereas no response could be linked to any company, the information obtained from the surveys could be used to generate aggregate summaries.

This survey had the highest number of respondents ever for an NRIC survey (Figure 3.3.4). The combined Focus Group 3A and Focus Group 3B respondents was 38.

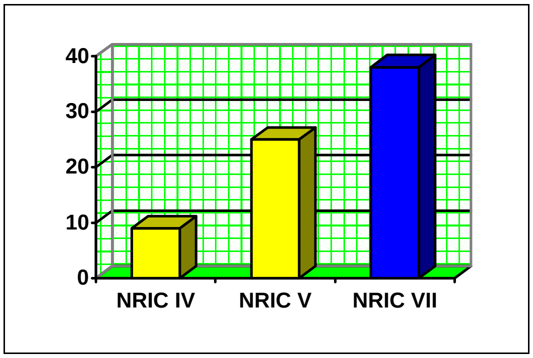


Figure 3.3.4. Improvement in Number of Survey Respondents.

The number of survey responses in NRIC VII for both the wireless and public data network companies was sufficiently large to support the statistical results and assessments that were reported. The results provide useful information on the

[44] The number of Best Practices in each survey was as follows: Service Provider and Network Operator - Wireless (65), PDN (67); Equipment Supplier – Wireless (42), PDN (38)

[45] For each Best Practice, respondents could select from the following choices: Effective, Moderately Effective, Not Effective, Don’t Know, and Not Applicable.

distribution of Best Practice responses, on the grouping and comparison of Best Practices and on the assessment of Best Practices by respondent category (e.g., wireless, public data network service providers). The participating companies were representative of the industry. Significant inroads were made in recruiting firms that were not NRIC members.

The public data network service providers and network operators that participated in the survey represent:

- Over 92% of the switched lines in-service in the US.
- Over 95% of the domestic wireline local, access and toll revenues.

The public data network equipment suppliers that submitted surveys:

- Account for the production of over 95% the circuit switches in-service in the US.
- Represent over 94% of the core routers shipped domestically.

3.3.5 Survey Results

The survey results are summarized in Table 3.3.5 below. The detailed adjustments from the learnings for each Best Practices are reported in the individual ingredient sections (Sections 2.2.1 to 2.2.8). Best Practices that were classified as “Ineffective” were reviewed by the Task Groups and either modified or deleted based on the comments received.

Table 3.3.5. Survey Results.

Number of Participants[46]	38
Number of Best Practices Surveyed	80
% of Best Practices Rated as Effective or Moderately Effective on Average	97%

3.3.6 Other Observations

There are two additional observations worth mentioning. The first is that the survey results indicated that there was strong agreement for those Best Practices rated as “Effective” (i.e., those that received this highest rating often did so by nearly everyone).

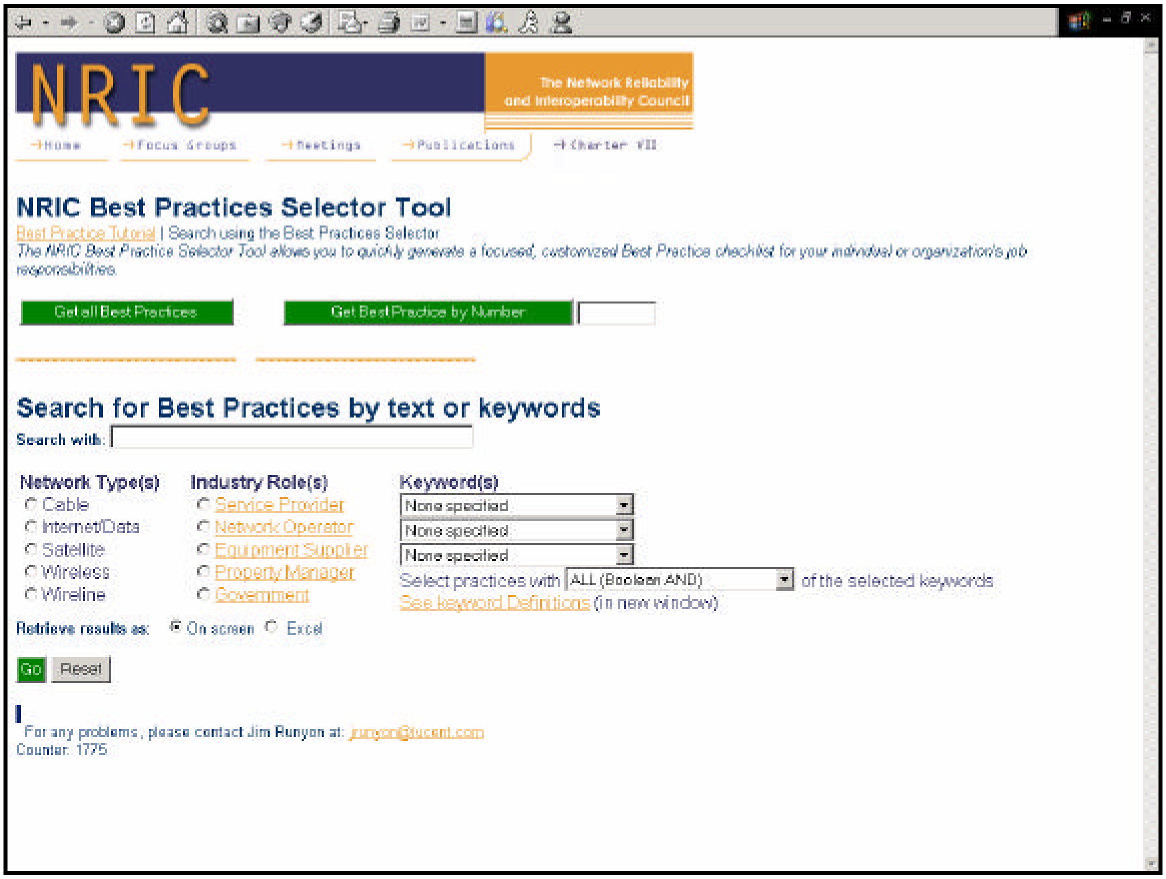
The second observation is that some Best Practices are identified by subject matter experts as being effective, and by other experts as being not applicable. This survey evidence further supports the principle that Best Practices are not applicable in all situations, as is stated throughout this report.

[46] For comparative purposes, represents the combined Focus Group 3A and Focus Group 3B survey; this represents a 52% improvement over NRIC V industry participation.

3.4 Best Practices

This section provides additional details on NRIC Best Practices that supplement those discussed in Section 2.3.2.

The NRIC Best Practices are maintained on the NRIC web site (www.nric.org). The NRIC Best Practice search page is shown below:



NRIC Best Practices Selector Tool

Best Practice Tutorial | Search using the Best Practices Selector

The NRIC Best Practice Selector Tool allows you to quickly generate a focused, customized Best Practice checklist for your individual or organization's job responsibilities.

Search for Best Practices by text or keywords

Search with:

Network Type(s)	Industry Role(s)	Keyword(s)
○ Cable	○ Service Provider	None specified
○ Internet/Data	○ Network Operator	None specified
○ Satellite	○ Equipment Supplier	None specified
○ Wireless	○ Property Manager	Select practices with ALL (Boolean AND) of the selected keywords
○ Wireline	○ Government	See keyword Definitions (in new window)

Retrieve results as: ● On screen ○ Excel

For any problems, please contact Jim Runyon at: jrunyon@lucent.com

Counter: 1775

Figure 3.4. NRIC Best Practices Selector Tool.

This web site provides a flexible means to retrieve NRIC Best Practices. The Best Practice selection options include:

- Selecting all Best Practices
- Selecting a specific Best Practice by number
- Searching for Best Practices containing a specified text
- Selecting Best Practices for Network Types (e.g., Wireless Networks)
- Selecting Best Practices based on Industry Roles (e.g., Service Provider)
- Selection using one to three Keywords

The following subsection provide a perspective on NRIC Best Practices developed by previous NRIC Councils, describes the intended use of Best Practices, describes the search options for the Best Practices, the methodology used to define Best Practices, and the Best Practice numbering scheme.

3.4.1 Best Practices and Previous Councils

Previous Councils provided Best Practices for the industry throughout their Final Reports. The earlier Councils focused on network reliability with particular attention to signaling and essential services; later Councils focused on interoperability. With the growing appreciation for their value in subsequent Councils, the Best Practices were increasingly drawn out of the reports as a distinct list. Also, the more recent Councils' scope for Best Practices expanded from traditional circuit switched technologies in wireline networks to wireless, cable and satellite networks as well as packet switched and converged solutions technologies.

The effectiveness of the NRIC Best Practices in preventing outages has been demonstrated consistently over the years. The ATIS NRSC has pointed out in its reports that most outages monitored at the national level could have been prevented if existing NRIC Best Practices had been implemented.[47] A thorough industry survey of the industry's implementation of NRIC V Best Practices was conducted in the second half of 2001. The results were reported in the NRIC V Network Reliability Best Practices Subcommittee Final Report. The results of this survey provide valuable insights into several dimensions of the industry's view of these Best Practices. The Fifth Council noted the following Key Learnings regarding the network reliability Best Practices from analysis of the industry survey:

- There is moderate to high risk to not implement the Best Practices
- There is usually not a high cost to implement the Best Practices
- The Best Practices are effective in preventing outages
- There is already a high level of implementation of the Best Practices[48]

3.4.2 Intended Use

Service providers, network operators, and equipment suppliers are encouraged to prioritize their review of these Best Practices and prioritize their implementation, as appropriate. As noted elsewhere in this report, the appropriate application of these Best Practices can only be done by individuals with sufficient knowledge of company specific network infrastructure architecture to understand their implications. Although the Best Practices are written to be easily understood, their meaning is often *not* apparent to those lacking this prerequisite knowledge and experience.

The NRIC Best Practices are intended to give guidance on how best to protect the U.S. communications infrastructure. Decisions of whether or not to implement a specific Best Practice are intended to be left with the responsible organization (e.g., Service Provider, Network Operator, or Equipment Supplier). Mandated implementation of these Best Practices is *not* consistent with their intent. As noted elsewhere in this report, the appropriate application of these Best Practices can only be done by individuals with sufficient knowledge of company specific network infrastructure architecture to understand their implications. Although the Best Practices are written to be easily

[47] NRSC Quarterly and Annual Reports provide detailed analyses of the industry's outage trends. The NRSC analysis of major network outages provides an understanding of the direct and root causes. These reports consistently find that existing NRIC Best Practices, if implemented, would prevent most of the major outages. www.atis.org

[48] Network Reliability Best Practices Subcommittee (2A.2) Presentation to the NRIC V Council and FCC at the FCC Building, January 4, 2002. www.nric.org.

understood, their meaning is often *not* apparent to those lacking this prerequisite knowledge and experience. Appropriate application requires understanding of the Best Practice impact on systems, processes, organizations, networks, subscribers, business operations, complex cost issues and other considerations. With these important considerations regarding intended use, the industry stakeholders are concerned that government authorities may inappropriately impose these as regulations or court orders. Because the NRIC Best Practices have been developed as a result of broad industry cooperation that engages vast expertise and considerable voluntary resources, such misuse of these Best Practices may jeopardize the industry's willingness to work together to provide such guidance in the future.

These Best Practices continue the theme stated over 10 year ago in the first NRIC (NRC) Report "Network Reliability: A Report to the Nation", also known as "The Purple Book").

> **"The Best Practices, while not industry requirements or standards, are highly recommended. The First Council stated, 'Not every recommendation will be appropriate for every company in every circumstance, but taken as a whole, the Council expects that these findings and recommendations [when implemented] will sustain and continuously improve network reliability.' "[49]**

The NRIC Best Practices continue to be developed consistent with this historic precedent.

3.4.3 Best Practice Search Options

The Best Practices can be retrieved by conducting a search using any of the following categories:

3.4.3.1 Industry Roles

Each Best Practice can have associations with any combination of five industry roles:

- Service Providers
- Network Operators
- Equipment Suppliers
- Government
- Property Mangers

3.4.3.2 Network Types

Each Best Practices is also associated with one of the following network types:

- Cable
- Internet/Data
- Satellite
- Wireless
- Wireline

[49] Executive Summary, NRIC V Best Practices Subcommittee Final Report, January 2002

3.4.3.3 Keywords

Keywords are not provided for every possible category that relates to Best Practices, but rather are provided to be as a means of helping the many users determine which Best Practices apply to their job responsibilities.

3.4.4 General, Previous Council and Historic References

The material in this section borrows heavily from the NRIC V Network Reliability Best Practices Subcommittee Report.

References can be a very important research tool for a user to determine applicability. References have been organized into three types:

- General
- Previous Council
- Historic

General references include citations or Web links to industry standards, white papers, or any other useful documentation. Previous Council references consist of the NRC I, NRC II, NRIC III, NRIC IV, NRIC V and NRIC VI Final Reports. Historic references include specific examples of outages (e.g., the 1988 Hinsdale Fire) that provide insights into how neglecting the associated Best Practice could have a substantial negative impact. Such information can be very important to a user considering the applicability of a set of Best Practices. This organizational structure of references has proven useful and is expected to provide better management of the insertion of future references. This capability provides substantial value to the users and is expected to result in ever increasing levels of implementation of Best Practices.

3.4.5 Best Practices Expressions

3.4.5.1 Basic Form

Most Best Practices have at their core a simple statement of the form:

"___ should ____, "

Where the first blank consists of any combination of Service Provider, Network Operator, Equipment Supplier, Property Manager, and Government. The second blank consists of the basic practice.

Such Best Practice sentences may be augmented with an "in order to . . ." statement that provides clarity as to the intent of the suggested action(s). This information may also be accessed, when available, on the web site.

There are also situations where the industry experts are aware that they are able to give very valuable guidance to the industry, but at the same time realize that the guidance would not fit every situation. The broad industry expertise often recognized that the vast diversity of networks and special conditions required some expression of understanding so as to not frustrate users of the Best Practices. In articulating the Best Practices, consistent with the work completed under previous Councils, the Focus Group met both objectives of (1) providing the valuable guidance, and (2) anticipating the diversity of circumstances, by using the following expressions to represent the flexibility needed by the industry:

“Should Consider”
This expression indicates that the subject should receive the guidance offered, but that implementation should be done only after carefully thinking through the benefits along with other considerations.

“As Appropriate, or When Appropriate, or Where Appropriate”
This expression indicates that the other factors need to be considered.

“When Feasible or Where Feasible”
This expression is similar to “As Appropriate”, except that it emphasizes the business or financial factors.

3.4.5.2 Critical Communications Infrastructure Facilities

Some Best Practices are intended for critical communications infrastructure. Because of the complex, sensitive and proprietary nature of this subject, critical communications infrastructure is defined by its owners and operators. Generally, such distinction applies to points of concentration, facilities supporting high traffic, and network control and operations centers, and equipment supplier technical support centers.

3.4.5.3 Numbering Format

Each NRIC Best Practice has a unique number that follows the numbering format:

X - Y - Z # # #

Where,
X = the current, or most recent, NRIC Council (i.e., 7 in 2004-2005)
Y = the Council in which the Best Practice was last edited (i.e., 7 for current work)
Z = 0-4 for Network Reliability (including Disaster Recovery & Public Safety)
= 1 for Disaster Recovery and Mutual Aid
= 3 for Mutual Aid
= 5 for Physical Security
= 8 for Cyber Security
= any digits, where every Best Practice has a unique Z # # #.

4 Conclusions

The Charter of the Seventh Council dedicated part of its focus to Network Reliability and included a focus on the public data network. The three deliverables identified by the NRIC VII charter were:

1. Identify gaps in existing NRIC Best Practices for the reliability of the Public Data Network.
2. Conduct an industry survey on the effectiveness of these Best Practices.
3. Modify existing Best Practices, and develop new Best Practices to address the specific needs of the Public Data Network.

4.1 Gap Analysis

The 11 gaps identified by this Focus Group were distributed across the infrastructure areas as follows:

Table 4.1. Distribution of Identified Gaps.

Area	Number of Gaps
Environment	1
Network	4
Power	2
Software	4

4.2 Effectiveness Survey

The Effectiveness Survey was completed on schedule. The following statistics summarize the survey results:

- 52% increase in the number of survey respondents (compared to NRIC V survey)
- 97% of Best Practices surveyed were rated as effective or moderately effective on average

In its analysis, the Focus Group observed that some Best Practices are identified by subject matter experts as being effective, and by other experts as being not applicable. This survey evidence further supports the principle that Best Practices are not applicable in all situations, as is stated throughout this report.

4.3 Public Data Network Best Practices

The number of new, modified or deleted Best Practices is identified in the following table.

Focus Group 3B PDN Summary of Best Practice Activities.

	Gap Closure Process (11 Gaps)	Effectiveness Survey Process	PDN Services Applicability Improvement Process	TOTAL
New Best Practices	26	0	19	**45**
Modified Best Practices	2	11	6	**19**
Deleted Best Practices	0	0	0	**0**

4.4 Areas for Further Investigation

In addition to completing the deliverables directed by the Council Charter, the Focus Group reviewed its work to determine if there were any discoveries that went beyond its scope, but that were appropriate to present. One such item was identified. The Power Task Group identified the following issue as one that is emerging as increasingly critical to the reliability of public data network services:

> The subject of power for residential and business premises equipment should be considered in future work, primarily as it relates to access to essential services during commercial power outages [Section 3.2.7].

4.5 Summary

The Focus Group completed all deliverables on time and consistent with the direction of the Council Charter. This report documents highly valuable guidance for service providers, network operators and equipment suppliers that promote the reliability for the nation's public data network.

5 Recommendations

Industry members are encouraged to continue their strong support to ensure sufficient expertise and resources are devoted to this task and the FCC is encouraged to provide a healthy, non-regulatory environment where industry experts can come together and develop Best Practices for voluntary implementation.

Going forward, industry participants are strongly encouraged to have their respective subject matter experts review these Best Practices for applicability. The NRIC web site (www.nric.org) Best Practices tools have keyword and other search capabilities that make identifying the list of applicable Best Practices to a given job function efficient. It is critical to note that Best Practices are not applicable in every situation because of multiple factors. Therefore, government entities are cautioned that mandating Best Practices could contribute to suboptimal network reliability or result in other negative consequences.

With this understanding, the Focus Group has prepared the following recommendation for the Council to advance these Best Practices:

> **The Council recommends that the NRIC VII Public Data Network Reliability Best Practices be implemented, as appropriate, by Service Providers, Network Operators and Equipment Suppliers, in order to promote the reliability and robustness of the public data network throughout the United States.**

These Best Practices have been developed to assure optimal reliability and robustness under reasonably foreseeable circumstances. The scope of this activity also encompasses guidance that promotes the sustainability of communications networks throughout the United States; the availability of adequate communications capacity during events or periods of exceptional stress due to natural disaster, terrorist attacks or similar occurrences; and the rapid restoration of communications services in the event of widespread or major disruptions in the provision of communications services.

Appendix 1. List of Interviewees

Focus Group 3B formed eight Task Groups corresponding to the different aspect of communications systems. Focus Group members and identified Subject Matter Experts participated in Task Groups as identified below.

NAME	COMPANY	ENVIRONMENT	HARDWARE	HUMAN	NETWORK	PAYLOAD	POLICY	POWER	SOFTWARE
Tim Hall	ALLTEL		L		X				
Rick Canaday	AT&T				X		X		
Victor DeVito	AT&T	X							
Howard Washer	BatteryCorp							X	
Jim Johnson	BellSouth		X						
Brent Austin	Century Telephone				X				
Robin Roberts	Cisco Systems		X						X
Dean Brewster	Comcast	L					X	X	
Mark Adams	Cox		X		L		X		
William Norton	Equinix				X		X		
Dave Cooper	Global Crossing				X				
Scott Bradner	Harvard Univ.		X		X		X	X	
Solos Arthachinda	IBasis					X			
Ajay Joseph	IBasis					X			
Ray Cruz	Internap	X						X	
Jim Fliers	Internap								X
David Frigeri	Internap					L			
Duke McMillan	Internap		X						X
Manny Sidhu	Internap					X			
Jon Vestal	Internap					X			X
Fred Stringer	Juniper		L						X
Rick Krock	Lucent	X	X					L	
Theodore Lach	Lucent		X						
Anil Macwan	Lucent			X					
Art Morrical	Lucent								X
Karl Rauscher	Lucent		L						
Jim Runyon	Lucent	L			X	X	X	X	X
Paul Wolfson	Lucent								X
Michael Diorio	MCI			X					

NAME	COMPANY	ENVIRONMENT	HARDWARE	HUMAN	NETWORK	PAYLOAD	POLICY	POWER	SOFTWARE
KC Kim	Nextel		X	L			X		
Brad Nelson	Quality & Reliability Solutions	X	X						L
Brian Rooks	Qwest	X			X		X		
Joe Provo	RCN				X		X		
Hank Kluepfel	SAIC		X						
John Chappa	SBC				X				
Ren Provo	SBC			X	X		X		
Molly Schwarz	Schwarz Consulting	X							
Chase Cotton	Sprint	X			X		L	X	

L = Leader
X = Participant

Appendix 2. Bibliography and Documentation

American National Standards Institute (ANSI): http://www.ansi.org/

ATIS Network Reliability Steering Committee (NRSC): http://www.atis.org

ATIS T1.320-1999 Central Office and Similar Facilities HEMP Standard.

ATIS T1.328-2000 Protection of Telecommunications Links, Baseline Standard

ATIS T1.333-19999 Above-Baseline Protection of Telecommunications Links.

ATIS T1E1.7 Baseline Electrical Protection for Towers and Bonding and Grounding for Commercial Buildings that House PSN Equipment.

ATIS T1E1.7 Physical Protection Standard for a Universal Telecommunications Equipment Mounting Frame for Central Offices.

CERT® Coordination Center (CERT/CC) for Internet Security: http://www.cert.org/advisories/CA-1998-01.html

CFR Title 47, Vol. 5, Part 215 (Assigns NCS responsibility as Federal lead on EMP technical data and studies relating to telecommunications).

Federal Communications Commission Code of Federal Regulations 47, 63.100.: http://www.fcc.gov

Hurst, N.W.; Immediate and underlying causes of vessel failures; Implications for including management and organizational factors in quantified risk assessment, Paper presented at IChemE Symposium Series No. 124, Institute of Chemical Engineers, Rugby, UK.

IEEE CQR, “Proceedings of the IEEE Technical Committee on Communications Quality & Reliability (CQR) 2001 International Workshop."

Internet Engineering Task Force (IETF): http://www.ietf.org

Internet Operators (IOPS): http://www.iops.org

Network Interconnection Interoperability Forum (NIIF): http://www.atis.org

North American Network Operators' Group (NANOG): http://www.nanog.org

National Communications System (NCS): http://www.ncs.gov

NRC I “Network Reliability: A Report to the Nation”, Alliance for Telecommunications Industry Solutions (ATIS), Washington, D.C. http://www.nric.org/pubs/index.html

NRC II Report: “Network Reliability – The Path Forward,” ATIS, February, 1996, Washington, D.C. http://www.nric.org/pubs/index.html

NRIC III Report: “NRIC Network Interoperability: The Key to Competition,” ATIS, July, 1997, Washington, D.C. http://www.nric.org/pubs/index.html

NRIC V Report, “The Future of our Nation’s Communications Infrastructure: A Report to the Nation,” January 4, 2002: http://www.nric.org

NRIC V Best Practices web site: http://www.nric.org

NRIC VI Best Practices web site: http://www/nric.org

Network Reliability Steering Committee (NRSC) Annual Reports: www.atis.org

Pat-Cornell, M.E., & Bea, R.G.; Management Errors and System Reliability: A probabilistic approach and application to offshore platforms, Risk Analysis, vol. 12, pp. 1 - 8, 1992.

T1 Standards Committee: http://www.nric.org

T1A1 Telecom Glossary: http://www.atis.or/tg2k

Telcordia Generic Requirements and Technical References: http://www.telcordia.com

Telcordia Generic Requirements (GR-63) - Network Equipment-Building System (NEBS) Requirements: http://www.telcordia.com

United States Department of State, Overseas Security Advisory Council, “Personal Security Guidelines For the American Business Traveler Overseas”, Department of State Publication10214, Bureau of Diplomatic Security, Released November 1994.

United States Department of State Travel Warnings and Overseas Security Advisory Council (OSAC): http://www.ds-osac.org/ and http://travel.state.gov/travel_warnings.html

United States Nuclear Regulatory Commission; FY 1991 Organization Factors Research and Applications Progress Report, US Nuclear Regulatory Commission Policy Issues, SECY-92-00, Jan. 1992.

Winsor, D. A.; Communications failures contributing to the challenger accident: An example for technical communicators, IEEE Transactions on Professional Communications, vol. 31, pp. 101-107, 1988.

Wireless Emergency Response Team (WERT) September 11, 2001 Terrorist Attacks on the New York City World Trade Center, October, 2001. www.wert-help.org.

Appendix 3. Acronyms

ANSI - American National Standards Institute
ATIS – Alliance for Telecommunications Solutions
ATM – Asynchronous Transfer Mode
AUP – Acceptable Use Policy
BCP – Business Continuity Plan
BGP – Boarder Gateway Protocol
BITS - Financial Services Roundtable
CIDR – Classless Inter-Domain Routing
CLEC – Competitive Local Exchange Carrier
CME – Coronal Mass Ejection
COMSOC - IEEE Communications Society
CQR – IEEE Technical Committee on Communications Quality & Reliability
CTIA - Cellular Telecommunications and Internet Association
C-TPAT – Trade Partnership Against Terrorism
DoS – Denial of Service Attack
DFO – Designated Federal Officer
DNS – Domain Name Server
EMI – Electro-Magnetic Interference
EMS – Element Management System
ERT – Emergency Response Team
ESD – Electro-Static Discharge
ESIF - Emergency Services Interconnection Forum
FACA – Federal Advisory Committee Act
FEMA – Federal Emergency Management Agency
FR – Frame Relay
FRU – Field Replaceable Unit
GETS – Government Emergency Telecommunications Service
FCC – Federal Communications Commission
GETS – Government Emergency Telecommunications Service
HEMP – High Energy Modulated Pulse
HVAC – Heating, Ventilation, and Air Conditioning
IEC - International Engineering Consortium
IEEE - Institute of Electrical and Electronics Engineers
IP – Internet Protocol
ISAC – Information Sharing and Analysis Center
ISP – Internet Service Provider
MIB – Management Information Base
NANOG - North American Network Operators' Group
NARUC - National Association of Regulatory and Utility Commissioners
NIST - National Institute of Standards and Technology
NCC – National Coordinating Center for Telecommunications
NCIC – National Crime Information Center
NCS – National Communications System
NIPC – National Infrastructure Protection Center
NNI – Network-to-Network Interface
NPSTC - National Public Safety Telecommunications Council

NRC – Network Reliability Council
NRIC – Network Reliability and Interoperability Council
NRSC – Network Reliability Steering Committee
NSIE – Network Security Information Exchange
NSTAC – National Security Telecommunications Advisory Committee
NS/EP – National Security and Emergency Preparedness
NTIA - National Telecommunications and Information Administration
NRIC – Network Reliability and Interoperability Council
OPASTCO - Organization for the Promotion and Advancement of Small Telecommunications Companies
OSHA – Occupational Safety and Health Administration
OSS – Operations Support System
PDN – Public Data Network
PSAP – Public Safety Answering Point
PSPTNS – Packet Switched Public Telecommunications Network Services
QoS – Quality of Service
RFC – Request for Comments
RFP – Request for Proposal
RPF – Reverse Path Forwarding
SDN – Software Defined Network
SLA - Service Level Agreement
SME – Subject Matter Expert
TCP/IP – Transfer Control Protocol/Internet Protocol
Telecom ISAC – Information Sharing and Analysis Center
USTA - United States Telecommunications Association
VPN – Virtual Private Network

Appendix 4. NRIC VII Charter

CHARTER
of the
NETWORK RELIABILITY and INTEROPERABILITY
COUNCIL – VII

A. The Committee's Official Designation

The official designation of the advisory committee will be the "Network Reliability and Interoperability Council VII" (hereinafter, the “Council”).

B. The Council's Objectives and Scope of Its Activity

The purpose of the Council is to provide recommendations to the FCC and to the communications industry that, if implemented, shall under all reasonably foreseeable circumstances assure optimal reliability and interoperability of wireless, wireline, satellite, cable, and public data networks.[50] This includes facilitating the reliability, robustness, security, and interoperability of communications networks including emergency communications networks. The scope of this activity also encompasses recommendations that shall ensure the security and sustainability of communications networks throughout the United States; ensure the availability of adequate communications capacity during events or periods of exceptional stress due to natural disaster, terrorist attacks or similar occurrences; and facilitate the rapid restoration of telecommunications services in the event of widespread or major disruptions in the provision of communications services. The Council shall address topics in the following areas:

1. Emergency Communications Networks Including E911

The Council shall report on ways to improve emergency communications networks and related network architectures and facilitate the provision of emergency services through new technologies.[51] This means ensuring that

[50] Public data networks are networks that provide data services for a fee to one or more unaffiliated entities

[51] Dale N. Hatfield concluded in *A Report on the Technical and Operational Issues Impacting the Provision of Wireless Enhanced 911 Services* that the current platform for E911 “has serious limitations in terms of speed, scalability, and adaptability. Additionally . . . these limitations not only burden the development of wireless E911 services, but . . . also constrain our ability to extend E911access to a rapidly growing number of non-traditional devices (e.g., PDAs), systems (e.g., telematics) and networks (e.g., voice networks that employ Voice-over-the Internet-Protocol – VoIP).”

emergency communications networks are reliable, survivable and secure. It also means that emergency communications networks (including E911[52]) can be accessed with currently available technologies as well as with new technologies (e.g., Voice-over-the Internet-Protocol (VoIP), text, pictures, etc., as appropriate).

The Council shall address the following topics:

a. Near Term Issues for Emergency/911 Services

The Council shall, by December 16, 2005 provide a report that contains near term emergency communications network Best Practices with supporting documentation.

In addition, the Council shall study specific issues that are identified below. The Council shall coordinate with other forums (e.g., Emergency Services Interconnection Forum (ESIF), National Emergency Numbering Association, etc.) so that each issue can be addressed as efficiently and completely as possible. The Council shall:

- Recommend accuracy requirements for location information particularly for rural, suburban, and urban areas and recommend ways to verify that accuracy requirements are met.[53] Investigate location technologies that could improve accuracy and/or reduce cost.

- Develop recommendations that will lead to a consistent format for information passed to Public Service Answering Points (PSAPs) for Phase 1 and 2 call and location information. This format must resolve any inconsistencies that would otherwise result from using vendor specific formats for transmitting information from Mobile Positioning Centers to PSAPs.

- Develop a consistent, common set of timing thresholds for the database queries and for obtaining location information.

- Specify the information that is to be sent to callers when major E911 network elements fail.

- Enumerate and evaluate the factors that should be considered in deciding whether redundant E911 tandems and alternate PSAPs should be provided to avoid a “fast busy” or a recorded message when one or more non-redundant network elements fail.

- Identify all major traffic concentration points in E911 architectures, such as E911 tandems, Selective Routing Databases (SRDB), Mobile Positioning Centers, and Automatic Location Identification (ALI) databases. The Council shall then define metrics and thresholds that should be used to determine where traffic concentrations are

[52] “E911” is an acronym for Enhanced 911 service.
[53] The work of ESIF Study Group G will be considered in this effort.

unacceptably high. The Council shall develop Best Practices to reduce traffic concentration wherever it has been determined to be too high. This includes developing Best Practices for the size and diversity of different databases. This may also include developing Best Practices aimed at improving the database process or reducing the number of database queries.

- Recommend ways to extend E911 services to satellite communications.

- Recommend ways to provide location information to PSAPs for calls originating from multi-line telephone systems (MLTS).

Interim Milestones

By December 17, 2004, the Council shall present a report recommending accuracy requirements for Phase 2 and ways by which compliance with these requirements can be objectively verified.

By April 4, 2005, the Council shall present a report recommending a consistent format for information that is to be passed to PSAPs for Phase 1 and 2 location information; and a consistent set of thresholds for the time required to complete database queries, and the metrics/thresholds for determining unacceptably high traffic concentration points.

By April 4, 2005, the Council shall present a report recommending the ways by which E911 services can be extended to satellite communications. That report shall also specify the information to be sent to the person originating the E911 call when major failures occur in E911 networks.

Final Milestone

By December 16, 2005, the Council shall present a report recommending ways and describing Best Practices to address near-term E911 issues. The report shall include issues from the earlier interim reports as well as recommend ways to extend E911 to MLTS. Finally, the report shall recommend Best Practices addressing high E911 network concentration points.

b. Long Term Issues for Emergency/E911 Services

The Council shall present a report recommending specific architecture properties that emergency communications networks are to provide by the year 2010 along with a generic network architecture that meets those properties. A set of architectures may be recommended depending on the characteristics of the area served. A plan as to how that architecture can be achieved, and how the current architecture can be evolved into the future architecture, shall be provided.

The Council shall:

- Recommend whether the Internet Protocol (IP) technology should be used to improve E911 services and, if so, how it may be used. In this regard, the Council shall address the future dependence of emergency communications networks on IP networks, and in particular, whether IP technologies should be used to get information to and from the PSAPs as communications networks continue to evolve. The potential use of IP to streamline the E911 network shall be addressed.

- Recommend what additional text and data information that emergency communications networks should be capable of receiving. This additional information may include text information (e.g., Instant messaging, e-mail, Short Message Service), pictures (e.g., from cellular phones), paging information, information from concierge services, Intelligent Vehicle Systems, automatic crash notification systems, etc. Recommend generic emergency communications network architecture(s) that will enable PSAPs to receive the recommended information.

- Recommend generic architecture(s) that will allow PSAPs to receive Voice-over-IP (VoIP) E911 calls and their associated call and location information.

- Recommend a long term strategy for processing overflow traffic from PSAPs.

- Recommend ways to modernize and improve the existing methods to access PSAPs (e.g., replacing Centralized Automatic Message Accounting (CAMA) trunks).

- Evaluate the feasibility and advisability of having a National/Regional PSAP to process overflow traffic efficiently from local PSAPs and to provide an interface for national security connectivity. Recommend whether the existing PSAP structure is adequate and whether alternate designs such as regional PSAPs should be explored.

Interim Milestones

By September 25, 2004, the Council shall present a report recommending the properties that network architectures must meet by the year 2010. These shall include the access requirements and service needs for emergency communications in the year 2010.

By June 24, 2005, the Council shall present a report recommending generic network architectures for E911 that can support the transmission of voice, pictures (e.g., from cellular telephones), data, location information, paging information, hazardous material messages, etc. The report shall describe how IP technology should be used.

By September 29, 2005, the Council shall present a report that identifies, in detail, the transition issues for the recommended generic network architectures and how the methods of accessing PSAPs should be modernized.

Final Milestone

By December 16, 2005, the Council shall present a final report describing the properties of the network architectures, the recommended generic network architectures, the transition issues, and the proposed resolutions of these transition issues along with recommended time frames for their implementation. The report shall also present conclusions on the feasibility and advisability of having a National/Regional PSAP and how the existing PSAP structure should be altered.

c. Analysis of Effectiveness of Best Practices Aimed at E911 and Public Safety

The Council shall determine the effectiveness of all Best Practices that have been developed to address E911 and Public Safety. The Council shall also:

- Analyze all outages related to E911 that have been reported pursuant to 47 C.F.R. § 63.100 and determine which Best Practices most clearly apply to E911 outages. The Council shall present recommendations on ways to reduce E911 outages. In addition it shall make recommendations on ways to improve the relevance of the FCC-Reportable Outage data for improving Emergency Communications. This includes defining direct causes and root causes which are better attuned to E911.

- Analyze 63.100 outages related to E911 to identify E911 architecture vulnerabilities.

- Make the language that is contained in the E911 NRC/NRIC Best Practices more precise so that E911 outages will be prevented and the level of compliance with each Best Practice can be reliably measured.

Interim Milestones

By September 25, 2004, the Council shall present a report containing its analysis of 63.100 outages related to 911/E911 and the Best Practices that are most applicable to E911 outages. The report shall also identify E911 architecture vulnerabilities.

By June 24, 2005, the Council shall present a report on its survey to determine how effective Best Practices have been for emergency communications.

Final Milestone

By December 16, 2005, the Council shall submit a report containing the newest version of each of the Best Practices for emergency communications. The report shall be based on its Best Practices survey and shall include revised language for the Best Practices to make them more precise. The report shall also summarize conclusions from its analysis of 63.100 outages.

d. Communication Issues for Emergency Communications Beyond E911

The Council shall present a report defining the long term network requirements for transmitting emergency services information emergency services personnel that is beyond the scope of E911 networks. E911 networks handle transmitting information from those originating E911 calls to PSAPs but not from PSAPs (or from some other network element) to emergency services personnel. The Council shall identify target architectures that will be able to transmit the needed information about the emergency event from PSAPs to emergency services personnel and to aid in coordinating emergency services activities. The Council shall also define the long term communication networks that shall be needed to transmit information from E911 calls to the Department of Homeland Security.

In this regard, the Council shall:

- Recommend whether IP architectures should be used for communications between PSAPs and Emergency Communications systems and personnel and, if so, how it may be used.

- Recommend how methods for accessing Emergency Services Personnel by PSAPs should be modernized.

- Recommend architectures that will allow PSAPs (or other network elements) to send text, pictures and other types of data, such as automatic crash information, to Emergency Services Personnel.

- Recommend the most appropriate role of 911/E911 in major disasters and for terrorist attacks.

Interim Milestones

By December 17, 2004, the Council shall present a report describing the properties that network architectures for communications between PSAPs and emergency services personnel must meet by the year 2010. These recommendations shall include the access requirements and service needs for emergency communications in the year 2010.

By September 29, 2005, the Council shall present a report that recommends the network architectures for communications between PSAPs and emergency service personnel that can support the transmission of voice, pictures (e.g., from a cellular phone), data, location information, paging information, hazardous material messages, etc. The report shall describe whether and how IP technology should be used.

By December 16, 2005, the Council shall present a report describing the transition issues for the recommended target architectures along with its recommended role for 911/E911 in major disasters and terrorist attacks.

Final Milestone

By December 16, 2005, the Council shall present a final report describing the properties of the target architectures for PSAP to emergency services personnel communications, the recommended network architectures, the transition issues, and a proposed resolution of these transition issues along with a time frame for their implementation.

2. Homeland Security Best Practices

By December 16, 2005, the Council shall present a final report that describes, in detail, any additions, deletions, or modifications that should be made to the Homeland Security Best Practices that were adopted by the preceding Council.

3. Best Practices for Wireless and Public Data Network Services

Building on the work of the previous Councils, as appropriate, this Council shall continue to develop Best Practices and refine or modify, as appropriate, Best Practices developed by previous Councils aimed at improving the reliability of wireless networks, wireline networks, and public data networks. In addition, the Council shall address the following topics in detail.

a. Best Practices for the Wireless Industry

The Council shall evaluate the efficacy of all Best Practices that have been developed for the wireless industry. The Council shall perform a gap analysis to determine areas where new wireless Best Practices are needed. The Council shall survey the wireless industry concerning the effectiveness of the Best Practices. The Council shall focus on the special needs of the wireless industry and refine existing Best Practices to focus their applicability to the wireless industry.

Interim Milestones

By December 17, 2004, the Council shall provide a report describing the results of the gap analysis of Best Practices aimed at the reliability of wireless networks.

By April 4, 2005, the Council shall complete its survey of the effectiveness of the Best Practices for the wireless industry.

Final Milestone

By September 29, 2005, the Council shall provide a report recommending the Best Practices for the wireless industry including the new Best Practices that particularly apply uniquely to wireless networks.

b. Best Practices for Public Data Network Services

The Council shall evaluate the applicability of all Best Practices that have been developed for public data network providers. The Council shall perform a gap analysis to determine areas where new Best Practices for these providers are needed. The Council shall survey providers of public data network services, including Internet data services providers, concerning the efficacy of existing Best Practices. The Council shall focus on the special needs of public data services providers and refine existing Best Practices to improve their applicability to Internet data services and other public data network services.

Interim Milestones

By December 8, 2004, the Council shall provide a report describing the results of the gap analysis of Best Practices aimed at the reliability of Internet data services.

By April 29, 2005, the Council shall complete its survey of the effectiveness of the Best Practices for Internet data services.

Final Milestone

By September 25, 2005, the Council shall provide a report recommending the Best Practices for Internet data services providers including the new Best Practices that particularly apply to public data network service providers.

4. Broadband

The Council shall present recommendations to increase the deployment of high-speed residential Internet access service. The Council shall include Best Practices and service features that are, and will be, technology-neutral. The Council's recommendations shall be prepared in such a way as: (1) to ensure service compatibility; (2) to facilitate application innovation; and (3) to improve the security, reliability and interoperability of both residential user systems and service provider systems.

C. Period of Time Necessary for the Council to Carry Out Its Purpose

The Council will have two years to carry out the purposes for which it was created.

D. Official to Whom the Council Reports

The Council shall report to the Chairman of the Federal Communications Commission.

E. Agency Responsible for Providing Necessary Support

The Federal Communications Commission will provide the necessary support for the Council, including the meeting facilities for the committee. Private sector members of the Council shall serve without any government compensation and shall not be entitled to travel expenses or per diem or subsistence allowances.

F. Description of the Duties for Which the Council is Responsible

The duties of the Council will be to gather the data and information necessary to submit studies, reports, and recommendations for assuring optimal communications services within the parameters set forth in Section B above.

G. Estimated Annual Operating Costs in Dollars and Staff Years

Estimated staff years that will be expended by the Council are three (3) for FCC staff and 12 for private sector and other governmental representatives. The Council's estimated operating cost to the FCC is $100,000 per year.

H. Estimated Number and Frequency of Council Meetings

The Council will meet at least three times per year. Informal subcommittees may meet more frequently to facilitate the work of the Council.

I. Council's Termination Date

Original filed on January 6, 1992; December 4, 1998 (amended); December 9, 1999 (renewed); December 26, 2001 (renewed); December 29, 2003 (renewed); April 15, 2004 (amended).

Appendix 5. Public Data Network Attributes

The following were proposed as PDN attributes during Focus Group discussions and do not represent consensus.

NETWORKS, STANDARD, OTHER

- Historic PDN: X.25, SMDS
- Many Protocols
- Should describe PDNs on a functional basis
    - o Do Not restricted PDNs to specific protocols (e.g., not just IP, ATM, SMDS)
    - o PDNs consist of:
        - o PAN – Public Access Network - do not discriminate but may have access requirements (i.e., may restrict access)
            - ▪ Not totally open to the public
                - AOL is a PAN
            - ▪ Provides Subscriber Access to Major Backbones [A 'stub' network – overused term]
            - ▪ 'Edge' Network
        - o (Pure) Transit Networks
            - ▪ Carries traffic from PANs
            - ▪ No Customer Access
        - o Core' Network
- PDNs have multiple personality disorder
    1) From consumer's perspective, the Internet (or PDAs) is a means to accessing content or services. Some of those services are communication tools, such as email and IM. Content is html based, streaming media or other sources. Another subset of content and services would include entertainment experiences, such as gaming.
    2) From the enterprise perspective, the Internet/PDAs is a connectivity tool, enabling communications between locations, clients, customers, etc. A huge component of this perspective includes a sales interface. Commerce portals and financial transactions are simply another storefront.
    3) The residual identity is comprised of research and other activities. However, only the above two components can be attributed to the growth and purpose that gives the Internet its life. In other words, we cannot have a discussion about the attributes of the Internet and yet ignore its identify.
- Internet, email services
    - Misconceptions: 'dial up' equals Internet
- Conglomeration of multiple physical layer platforms (ATM, Frame)
- Shared Network (vs. closed)
- Access Agnostic

APPENDIX 5 (cont'd)

- Multiple Physical Layers (transport):
  - Copper
  - Fiber
  - Wireless (e.g., WiFi)
  - Free Space Optics
- Security depends on both the public and private networks
- PDN can be characterized by the OSI reference model
  - Many items defined in Stack Layers
- Addressing Global For example, Best Practices that recommend avoiding the placement of critical network facilities in high risk areas could, *if followed without appropriate consideration*, result in poor coverage. Similarly, a Best Practice that encourages deployment of certain types of back-up power, *if implemented inappropriately*, could result in a violation of local ordinances. And, likewise, a Best Practice that encourages the removal of foliage near infrastructure in some instances may result in deterioration or destruction of environmental aesthetics if proper discretion is not used.
- Public
- Networks
- Data
- A 'Transmission Media' that is not application sensitive
- Service Characteristics
  - Performance, Security, Reachability, Network *Accessibility*
- Applications & Services that <u>often</u> attempt to fairly share resources
- Known address space vs. unknown address space
- Inter-carrier relationships are common
- Addressing with <u>Routing Mechanism</u> (BGP, other)
- Often under multiple administrative domains / authorities
- IP Address space is globally shared (assigned) – under RIR (Regional Internet Registry - addressing authorities)
- Internet applications are functionally dependent on DNS
- Uncertain Jurisdiction (global nature)
- Internet is Decentralized
- Often Any-to-Any
- Performance Characteristics
  - Today – driven by Market Demand
    - + Sal's /performance characteristics
    - + *Obsolete:* PDN are 'best effort'
  - 5 9's are 'port availability' are SLA driven
  - Latency, Loss, and Jitter are Network wide characteristics
  - Public Slaps are not the same as SLA

- Blurring of Reliability and Quality
- Connection-less (IP) and Connection-orientated
- Different <u>expectation</u> for different service applications
  - Phone vs. Email (gap is closing)
- Evolving
- Convergence

APPENDIX 5 (cont'd)

- Transition to an all digital & packet network
- Various/Different 'starting points'
- Trouble Shooting PDN
  - End User has visibility to global infrastructure (e.g., Ping/Trace Routes)
  - Requires secure management of network elements (e.g., SNMP data)
  - Multiple administrative entities are often involved in problem resolution
    - Provider of the infrastructure
    - Customer facing trouble shooting
    - 3rd Party Partner (Peering, Data Center, Network-to-Network Interfaces)
    - On-Net / Off-Net
    - Provider of the connectivity to the Internet
    - (Possible end-user)
- High growth rate
  - Increasing demand
- Increasing Dependence of Public Safety, National Security, Financial Stability on PDNs
- Effective use of PDNs are a competitive advantage to individual corporations
  - Reduce cost of operations
  - Speed up delivery of new services
- Different statistical daily traffic patterns than PSTN
- Aggregate traffic profile is predictable (daily, monthly, yearly)
- Instantaneous real time statistical traffic patterns unpredictable (i.e., connectionless networks)
- Challenging for statistical abnormalities in traffic (i.e., connectionless networks)
- Any-to-Any characteristic of the PDN makes vulnerable to DDoS
  - Complicates traffic management
- Intelligence of the network is being pushed to the edge of the network
- Points of Infrastructure concentration (e.g., Telcom Hotels, Fiber right-a-ways)
- Property Managers play a key role in controlling the environment (e.g., power upgrades)
- Varying standards for building and network equipment
- Testing fail-over emergency and escalation plans are vital in light of rapid growth/change (e.g., evolving and upgrading power)

PAYLOAD

- Internet is A Network of Networks (BGP is the existing mechanism)
- Often combine signaling and payload

SOFTWARE

- Network Element software reliability is crucial
- SW upgrades require interoperability testing

HARDWARE

- Increasing use of same hardware (integrated circuits) in the equipment
- Trend of outsourcing for HS/SW

APPENDIX 5 (cont'd)

POWER

- Design with redundant power is relatively new
- Lack of data to monitor power outages (e.g., cable remotes)
- DC or AC power
- On-site end-user power is required to work
- End-user power may be regulated

HUMAN

- Physical and cyber access to the control of the networks is not limited to few people (e.g., human error, malicious intent)
- Significant skill is required to design, configure, maintain, operate PDNs
- Increased trend to customer self service (i.e., automated self help)
- PDNs are highly ubiquitous?
- Wide variety of applications (voice, video, …)

POLICY / REGULATORY ASPECTS Include:

- Often unregulated
- Varied regulation
- Support for Critical/Essential Services
- No Universal Access Mandate
  - QoS of Applications
  - Undefined PDN Emergency Services
    - E911?
    - Legally required to provide?
  - VoIP
- Primary vs. Secondary Line Treatment/Priority
- Emerging Lawful Intercept Requirements (CALEA)
  - Expectations of User?
  -

****

Other Contributions
(Not PDN Attributes)

- No fundamental security in PDN
- Security – corporate vs. public network and secure the network (all layers)
- "Internet Focus" (IP)
  - Below - Infrastructure
  - Above - Applications
- Focus on Layer 3 (not layers below)
- Internet requires BGP
- Mechanisms that encourage Private Address Space
- PDN reliability depends on upper layers for data integrity
- PDN is fundamentally an unreliable network
  - New Protocols address this
  - Reliability is enhanced above layer 3

Appendix 6. Public Data Network Gaps

The 11 gaps identified by the PDN Focus Group are:

- **Environment Gap**

  Managing Growth in Multi-Tenant Facilities

  The Environment Task Group identified one gap in existing, NRIC Best Practices related to the complexity of managing growth in third party and multi-tenant environments (e.g., space, power, cooling).

- **Network Gaps**

  Four Network Gaps have been identified:

  Network Design and Planning

  73 Best Practices currently exist relative to network design. The Task Group has identified opportunities to enhance NRIC Best Practices in the following areas: the treatment of private address space, routing practice, and design audit.

  Network Measurement and Management

  One Best Practice exists relative to Equipment Suppliers measuring and improving quality. The Task Group has identified opportunities to expand and clarify the scope of the Best Practice to include Service Providers and Network Operators.

  Network Spares Administration

  At least 12 current Best Practices touch on spare equipment. The Task Group has identified an opportunity to improve guidance in the area of spares management.

  Maintenance Window

  One current Best Practice exists for the definition of maintenance windows. The Task Group has identified an opportunity to improve guidance in the communication of maintenance timeframes.

- **Power Gaps**

  Proper Identification of Cables

  Administration, maintenance and operations of network elements depend on proper identification of equipment. While there are numerous Best Practices that address administration, operations and maintenance, and while Network Operators currently employ various effective methods of cable labeling, the NRIC Best Practices do not document guidance in this area.

  Back-Up Power for On-Premise Emerging Data Services Equipment

  Emerging data services, such as Voice Over IP (VoIP) are increasingly viewed as critical services. As such, this equipment may need to continue to function even during commercial power outages. Because the end user equipment is increasingly powered by local sources, back-up power consideration should be explored. As these networks are still very new, further analysis is pending.

- **Software Gaps**

Management Information Base (MIB)

Due to the quantity and interactions of "private" MIB extensions with proprietary and other management software, the Task Group has identified opportunities to enhance NRIC Best Practices in the areas of MIB support, standardization, and documentation. In addition, there is opportunity to improve support of environmental variables in MIBs.

Crash Diagnostic Memory

The Task Group has identified opportunities to enhance NRIC Best Practices in the area of crash diagnostic memory storage and the use non-volatile memory. There is added opportunity to improve storage of core dumps and system states associated with a crash.

Software Configuration

The Task Group has identified opportunities to enhance NRIC Best Practices in the area of software configuration change management and version control. There is also an opportunity to improve change management documentation, revision change history, and source material. In addition, there is a need for guidance in the area of software production standards affecting software configurations and software back-ups. Finally, there is an opportunity to enhance Best Practices in the area of manual and automated software configurations impacting installation and back-out procedures, change tools, upgrades, and limited/phased deployments.

Test Environment Descriptions and Published Capacity

The Task Group has identified opportunities to enhance NRIC Best Practices in the area of test environment descriptions along with the use of "published" capacity in software testing and qualification.

Appendix 7. PDN Modifications of Existing Best Practices

BP Number	Best Practice	Reference / Comments
7-P-0515	**Role-based Mailbox:** Network Operators and Service Providers should, for easy communication with subscribers and other operators and providers, use specific role-based accounts (e.g., abuse@provider.net, ip-request@provider.net) versus general accounts (e.g., noc@provider.net) which will help improve organizational response time and also reduce the impact of Spam.	
7-P-0516	**Route Flapping:** Network Operators and Service Providers should manage the volatility of route advertisements in order to maintain stable IP service and transport. Procedures and systems to manage and control route flapping at the network edge should be implemented.	
7-P-0517	**Equipment Control Mechanisms:** Equipment Suppliers should design network elements and associated network management elements with the combined capability to dynamically handle peak load and overload conditions gracefully and queue and shed traffic as necessary (e.g., flow control).	The management of peak load and overload conditions can apply to bearer traffic, signaling traffic, routing and control protocol traffic, network management traffic/messaging, accounting statistics, and flow reporting.
7-P-0518	**Capacity Monitoring:** Network Operators should design and implement procedures for traffic monitoring, trending and forecasting so that capacity management issues may be understood.	NRIC VII split this BP into two parts. See BP 0616 for 'Failure Effects Analysis'
7-P-0519	**Capacity Monitoring:** Network Operators and Service Providers should engineer and monitor packet networks to ensure that operating parameters are within capacity limits of their network design (e.g., respect limitations of deployed packet switches, routers and interconnects, including "managed networks" and "managed CPE"). These resource requirements should be re-evaluated as services change or grow.	

BP Number	Best Practice	Reference / Comments
7-P-0521	**Industry Standards:** Network Operators, Service Providers and Equipment Suppliers should work toward implementing industry standards for interconnection points (e.g., IETF, applicable ANSI T-1 standards).	The current environment of numerous Network Operators, Service Providers and Equipment Suppliers elevates the importance standards adoption (e.g., IETF and ITU-T standards).
7-P-0522	**Industry Forum Participation:** Network Operators, Service Providers, and Equipment Suppliers should participate in standards development organizations and industry forums.	The current environment of numerous Network Operators, Service Providers and Equipment Suppliers elevates the importance of industry dialogue and standards (e.g., IETF, ITU-T, NANOG, NRIC).
7-P-0532	**Diversity Audit:** Network Operators should periodically audit the physical and logical diversity called for by network design and take appropriate measures as needed.	
7-P-0548	**Post Mortem Review:** Service Providers and Network Operators should have an internal post mortem process to complete root cause analysis of major network events with follow-up implementation of corrective and preventive actions to minimize the probability of recurrence. Network Operators and Service Providers should engage Equipment Suppliers and other involved parties, as appropriate, to assist in the analysis and implementation of corrective measures.	
7-P-0603	**Schedule System Backups:** Network Operators and Service Providers should establish policies and procedures that outline how critical network element databases will be backed up onto a storage medium (e.g., tapes, optical diskettes) on a scheduled basis.	Examples of network databases include router configurations, digital cross connect system databases, switching system images, base station controller images. These policies and procedures should address, at a minimum, the following: Database backup schedule and verification procedures; Storage medium standards; Storage medium labeling; On site and off site storage; Maintenance and certification; Handling and disposal.

BP Number	Best Practice	Reference / Comments
7-P-0607	**Inter-Provider Fault Isolation:** Network Operators and Service Providers should ensure that bilateral technical agreements between interconnecting networks address the issue of fault isolation.	At a minimum, these agreements should address the escalation procedures to be used when a problem occurs in one network. The agreement should also address what information will be shared between the interconnected companies.
7-P-0614	**Equipment Identification:** Service Providers, Network Operators and Equipment Suppliers should position the equipment designation information (e.g., location, labels, RFID tags) so that they are securely affixed. The equipment designation should not be placed on removable parts such as covers, panels, doors, or vents that can be removed and mistakenly installed on a different network element.	
7-P-0616	**Failure Effects Analysis:** Network Operators should design and implement procedures to evaluate failure and emergency conditions affecting network capacity.	NRIC VII split this BP into two parts. See BP 0518 for 'Capacity Monitoring'
7-P-0617	**Route Controls:** Network Operators and Service Providers should ensure that routing controls are implemented and managed to prevent adverse routing conditions.	Adverse routing conditions may include such things as infinite looping and flooding of datagrams across data networks. Controls should be implemented across network boundaries to limit the frequency of route advertisements and prevent routing of reserved or private address space. Controls should also prevent unauthorized advertisements of other operators' address space that is not legitimately allocated or assigned to the proper entity. For example, see those addressed in RFC 1918 - http://www.ietf.org/rfc/rfc1918.txt.
7-P-0645	**HVAC Maintenance:** Network Operators, Service Providers and Property Managers should inspect and maintain heating, venting, air conditioning (HVAC) areas.	

BP Number	Best Practice	Reference / Comments
7-P-5058	**Back-up Power:** Service Providers, Network Operators, Equipment Suppliers and Property Managers should ensure that all critical infrastructure facilities, including the security equipment, devices and appliances protecting it, are supported by backup power systems (e.g., batteries, generators, fuel cells).	
7-P-5075	**Network Diversity:** Network Operators and Service Providers should ensure that networks built with redundancy are also built with geographic separation where feasible (e.g., avoid placing mated pairs in the same location and redundant logical facilities in the same physical path).	
7-P-5084	**Hardware & Software Quality Assurance:** Service Providers, Network Operators and Equipment Suppliers should consider ensuring that outsourcing of hardware and software includes a quality assessment, functional testing and security testing by an independent entity.	Independent entities do not include the source supplier. Quality and security testing may include the following: GR929 (RQMS), GR815, TL9000.
7-P-5196	**MOPs:** Service Providers and Network Operators should ensure that contractors and Equipment Supplier personnel working in critical network facilities follow the current applicable MOP (Method of Procedures), which should document the level of oversight necessary.	
7-P-8061	**IR (Incident Response) Procedures:** Service Providers and Network Operators should establish a set of standards and procedures for dealing with computer and network security events. These procedures can and should be part of the overall business continuity/disaster recovery plan. Where possible, the procedures should be exercised periodically and revised as needed. Procedures should cover likely threats to those elements of the infrastructure which are critical to service delivery/business continuity. See Appendix X and Y.	

Appendix 8. PDN New Best Practices

BP Number	Best Practice	Reference Column
7-P-0400	**Network Performance Measurements:** Service Providers and Network Operators should establish measurements to monitor their network performance.	Reference industry guidelines such as applicable ITU, Telcordia, TL9000 standards for assistance in setting measurements on availability and reliability for criteria to measure quality of service (e.g., delay, loss, port availability, jitter).
7-P-0401	**Network Surveillance:** Service Providers and Network Operators should monitor the network to enable quick response to network issues.	
7-P-0402	**Single Point of Failure:** Service Providers and Network Operators should, where appropriate, design networks to minimize the impact of a single point of failure.	
7-P-0403	**Maintenance Notification:** Service Providers and Network Operators should communicate maintenance windows to their customers.	
7-P-0404	**Network Performance:** Service Providers, Network Operators and Equipment Suppliers should incorporate methodologies that continually improve network or equipment performance.	Also, see BP 0802
7-P-0405	**Network Performance:** Service Providers and Network Operators should periodically examine and review their network to ensure that it meets the current design specifications.	
7-P-0406	**Spares and Inventory:** Service Providers and Network Operators should, where appropriate, establish a process to ensure that spares inventory is kept current to at least a minimum acceptable release (e.g., hardware, firmware or software version).	

BP Number	Best Practice	Reference Column
7-P-0407	**NOC Communications:** Network Operators and Service Providers should establish processes for NOC-to-NOC (Network Operations Center) peer communications for critical network activities (e.g., scheduled maintenance, upgrades and outages).	
7-P-0408	**Ingress Filtering:** Service Providers and Network Operators should, where feasible, implement RFC 3704 (IETF BCP84) ingress filtering.	
7-P-0409	**Routing Resiliency:** Service Providers should use virtual interfaces (i.e., a router loopback address) for routing protocols and network management to maintain connectivity to the network element in the presence of physical interface outages.	
7-P-0410	**Security Services and Procedures:** Service Providers and Network Operators should, as appropriate, review, understand, and implement "Internet Service Provider Security Services and Procedures" (RFC3013/BCP46).	
7-P-0411	**Cable Management:** Network Operators and Service Providers should consider developing and implementing cable labeling standards.	See Telcordia GR-1275 (Installation Standards Manual)" references.
7-P-0412	**IP Element Security:** To enhance security, Network Operators and Service Providers should, by default, disable ICMP (Internet Control Message Protocol) redirect messages and IP source routing.	ICMP - Internet Control Message Protocol
7-P-0413	**Maintenance Notification:** Service Providers and Network Operators should communicate information on service affecting maintenance activities and events to their customers, as appropriate.	
7-P-0414	**Maintenance Notification:** Service Providers and Network Operators should establish plans for internal communications regarding maintenance activities and events that impact	

BP Number	Best Practice	Reference Column
	customers.	
7-P-0415	**Data Back-up Verification:** Network Operators and Service Providers should test the restoral process associated with critical data back-up, as appropriate. The goal is to demonstrate that data restoration is complete and works as expected.	
7-P-0416	**Capacity Management:** Network Operators should design and implement procedures for traffic monitoring, trending and forecasting so that capacity management issues may be addressed.	
7-P-0417	**Capacity Management:** Network Operators should design and implement procedures to evaluate failure and emergency conditions affecting network capacity.	
7-P-0418	**Back-out MOPs:** Service Providers and Network Operators should, where appropriate, have a documented back-out plan as part of a Method of Procedure (MOP) for scheduled and unscheduled maintenance activities.	
7-P-0419	**Capacity Management Systems:** Service Providers should design and capacity-manage EMSs (Element Management Systems) and OSSs (Operational Support Systems) to accommodate changes in network element capacity.	
7-P-0420	**Management Systems Performance:** Network Operators should periodically measure EMS (Element Management System), NMS (Network Management System) and OSS (Operational Support System) performance and compare to a benchmark or applicable requirements to verify performance objectives and expectations (e.g., internal performance criteria, system vendor specifications) are being met.	

BP Number	Best Practice	Reference Column
7-P-0421	**Fast Failover of Redundancies:** Equipment Suppliers should design network elements intended for critical hardware and software recovery mechanisms to minimize restoration times.	Common recovery mechanisms could include the fail-over to: a) the redundant hardware components (modules, FRUs), b) redundant and/or backup software processes, c) switch to alternate paths, circuits or virtual circuits, and, d) switch to redundant or backup storage of system data.
7-P-0423	**Cable Management:** Equipment Suppliers should provide cable management features and installation instructions for network elements that maintain cable bend radius, provide strain relief and protection from cable damage, while also leaving clear access for cable rearrangement (i.e., moves/add/deletes) and FRU (Field Replaceable Unit) swaps.	
7-P-0424	**Electrical Safety Standards:** Network Operators should identify and require applicable safety standards for network elements that they plan to purchase, procure or implement. Recognized standards should be used where ever possible, with specific requirements cited rather than statements such as UL Listed or NEC compliant.	Recognized standards may include UL, NEC, ANSI, NFPA, ASTM. Specific requirements such as "UL-498/NEC-250.146(A)-Receptacle Grounding-Surface-Mounted Box."
7-P-0425	**Software Management:** Service Providers and Network Operators should maintain software version deployment records, as appropriate.	
7-P-0426	**Software Change Control:** Equipment Suppliers should use software change control to manage changes to source material used in the production of their products.	Ref: As such, the software change control system used by equipment suppliers should be able to manage both ASCII and binary (source object code) files.
7-P-0427	**Software Documentation:** Equipment Suppliers should maintain software documentation including revision change history and associated release notes.	

BP Number	Best Practice	Reference Column
7-P-0428	**Software & Hardware Vulnerability Tracking:** Service Providers should monitor software and hardware vulnerability reports and take the recommended action(s) to address problems, where appropriate. These reports and recommendations are typically provided by equipment suppliers and CERTs (Computer Emergency Response Teams).	
7-P-0429	**Crash Diagnostics:** Equipment Suppliers should provide appropriate storage and retrieval mechanisms for diagnostics after a hardware or software crash.	Information useful for diagnostics might include core dumps and register contents.
7-P-0430	**Software Configurations**: Equipment Suppliers should be able to recreate supported software from source and, where feasible, software obtained from third parties.	
7-P-0431	**Capacity and Performance Data:** Equipment Suppliers should provide capacity and performance data for network elements.	Use commonly agreed upon terminologies and methodologies such as those developed by IETF Benchmarking Methodology Working Group (e.g., RFC 2544).
7-P-0432	**Standardized MIBs:** Equipment Suppliers should support standardized MIBs (Management Information Bases) and maintain documentation of private and enterprise MIBs.	Enterprise MIBs are those written by vendors for their particular object. The managed object can furnish both standard MIB and enterprise MIB information. The standard MIBs are those that have been approved by the IAB (Internet Architecture Board, www.iab.org). Equipment and software vendors define the private MIBs unilaterally.
7-P-0433	**MIB Environment Variables:** Equipment Suppliers should support, clearly define and document environmental variables in Management Information Bases (MIB).	MIB Environmental variables include the location of hosts, servers, terminals and other nodes as well as the traffic for the object.

BP Number	Best Practice	Reference Column
7-P-0434	**Employee Training:** Service Providers, Network Operators, Equipment Suppliers and Property Managers should provide appropriate training and periodic refresher courses for their employees.	
7-P-0435	**ID Network Reliability Functions:** Service Providers, Network Operators, Equipment Suppliers and Property Managers should assess the functions of their organization and identify those critical to ensure network reliability.	
7-P-0436	**Problem Handling Continuity:** Service Providers should have a process to ensure smooth handling and clear ownership of problems that transition shifts or organizational boundaries.	
7-P-0437	**Route Aggregation:** Network Operators and Service Providers should aggregate routes where appropriate (e.g., singly-homed downstream networks) in order to minimize the size of the global routing table.	
7-P-0438	**CIDR Use:** Network Operators and Service Providers should enable CIDR (Classless Inter-Domain Routing) by implementing classless route prefixes on routing elements.	
7-P-0439	**BGP Authentication:** Network Operators and Service Providers should authenticate BGP sessions (e.g., using TCP MD5) with their own customers and other providers.	
7-P-0440	**Route Exchange Limits:** Network Operators and Service Providers should set and periodically review situation-specific limits on numbers of routes imported from peers and customers in order to lessen the impact of misconfigurations.	

BP Number	Best Practice	Reference Column
7-P-0441	**Unicast RPF:** Network Operators and Service Providers should, where feasible, implement Unicast RPF (Reverse Path Forwarding) to help minimize DOS attacks that use source address spoofing.	
7-P-0442	**End-to-End Path Monitoring:** Service Providers should consider measuring end-to-end path performance and path validity for both active and alternate routes	
7-P-5282	Service Providers should coordinate with Property Managers to ensure adequate growth space.	
7-P-5283	Equipment Suppliers should provide network element thermal specifications or other special requirements in order to properly size Heating, Ventilation, and Air Conditioning (HVAC) systems.	

Appendix 9. Acknowledgements

The Focus group leaders recognize the following:

Participating Companies
The organizations that sent technical experts are recognized for their vital support. Without the commitment of such companies to the reliability of the nation's Public Data Network, this work could not have been completed.

Task Group Leaders
The development of industry consensus required significant leadership and attention to a wide variety of concerns and interests. The Task Group leaders provided much of this talent and energy.

Task Group Members
The technical contributions and diligence in participating in industry consensus development is highly commendable. In many instances, members dedicated significant personal time to support the completion of the team's mission.

Other Experts
Countless other subject matter experts were engaged both from participating companies and other members of the public data network community. Their insights provided additional strength to the Task Group's competence.